# CHAPTER 5

# GENERAL SECURITY

## LEARNING OBJECTIVES

*Upon completing this chapter, you should be able to do the following:*

- *Identify the procedures for verifying the identification and clearance of recipients.*
- *Identify the procedures for TEMPEST requirements.*
- *Identify methods of controlling access to security areas, including designation of restricted areas, requirements relating to lock combinations, and procedures for sanitizing sites and equipment.*
- *Identify the procedures and regulations for marking material and conducting inventories of classified material (Secret and below).*
- *Identify the procedures used for clearing media and hardware of classified material (Secret and below).*
- *Identify the regulations and procedures for declassification or destruction of classified hardware and the destruction of classified material (Secret and below).*
- *Identify the regulations and procedures covering the receipt, inspection, handling, destruction, and verification of classified material (SPECAT or Top Secret and above).*

---

Your duties as a Radioman will require that you handle considerable amounts of classified information and equipment. You should be able to recognize classified matter and know what to do—or not do—with it. Security is as basic a part of your assignment as operating telecommunications equipment. Safeguarding classified information is an integral part of your everyday duties.

The security of the United States in general, and of naval operation in particular, depends upon the safeguarding of classified information. As a Radioman, you will learn information of vital importance to both the military and the nation. At times, vast amounts of classified message information will pass through your hands.

You must be security conscious to the point that you automatically exercise proper discretion in the discharge of your duties. In this way, security of classified information becomes a natural element of every task and not an additionally imposed burden.

## RECIPIENT'S IDENTIFICATION AND CLEARANCE

Identification may be provided with the member military identification card, command identification cards or badges. Normally, local standard operating procedures cover the individual command's requirements. Guidelines for identification and access are contained in the *Department of the Navy Information and Personnel Security Program*

*Regulation*, OPNAVINST 5510.1, hereinafter called the *Security Manual.*

- Military identification cards are required to be carried by all active duty military. They aid only in recognizing the individual, not access or clearance.
- A command identification card/badge assists in identifying the level of security clearance of the holder or where the holder is authorized to enter. These cards/badges are only an aid and may not be used as the basis for granting access to information or areas.

A personnel security clearance will be issued to an individual by the Department of the Navy Central Adjudication Facility (DONCAF), or other designated clearance authority with favorable completion of required paperwork in accordance with the *Security Manual*. A copy of OPNAV 5510/413 (Clearance Report) will be filed in the member's permanent service record and in the security officer's files.

## CONTROL OF COMPROMISING EMANATIONS (TEMPEST)

Compromising emanations (CE), referred to as "TEMPEST," are unintentional data-related or intelligence-bearing signals. If these signals are intercepted and analyzed, they could disclose the information transmitted, received, handled, or otherwise processed by electrical information-processing equipment or systems. Any electrical information-processing device, whether an ordinary electric typewriter or a large complex data processor, may emit compromising emanations.

### TEMPEST VULNERABILITY ASSESSMENT (TVA)

The vulnerability of a ship, aircraft, shore station, transportable equipment, or a contractor facility is determined by a TEMPEST Vulnerability Assessment. This assessment includes each of the following factors, which, together, create vulnerability:

**Susceptibility—** The probability that TEMPEST signals exist and are open to exploitation.

**Environment—** The primary environmental considerations are the geographical location of a ship, aircraft, shore station, or contractor facility; physically and electrically controlled spaces; adherence to approved installation criteria; and the use of TEMPEST-approved equipment or systems.

- **Threat—** The capability and motivation of an enemy to exploit the TEMPEST signal.

The interaction of all of these factors determines the vulnerability. From this assessment and considering the category, classification, or sensitivity of the information involved, a determination will be made. An Instrumented TEMPEST Survey (ITS) will be scheduled, or the requestor will be placed in the "acceptable risk" category.

### Tempest Vulnerability Assessment Request (TVAR)

A TVAR must be submitted prior to processing classified data. This request should be sent to the Naval Criminal Investigative Service, Washington D.C., with a copy to CO, NAVELEXSECCEN and other commands as appropriate. The list of required information is available in *Navy Implementation of National Policy on Control of Compromising Emanations (U)*, OPNAVINST C5510.93.

Some ships are identified by CNO as high TEMPEST risk platforms. Those which are likely to be the target of hostile TEMPEST collection efforts will be scheduled for an Instrumented TEMPEST Survey (ITS). No TVAR is required from any ship.

### EMISSION CONTROL (EMCON)

EMCON is used to prevent an enemy from detecting, identifying, and locating friendly forces. It is also used to minimize electromagnetic interference among friendly systems. EMCON is normally imposed by a commander to control all electromagnetic radiations. Once EMCON is imposed, general or specific restrictions may be added to the EMCON order, depending on the operational, intelligence, or technical factors for the area affected.

For radiomen, EMCON usually means either full radio silence or HF EMCON. The most secure communications methods during EMCON reduce, but do not eliminate, the possibility of identification. It is assumed that any electromagnetic radiation will be immediately detected, and the position of the transmitting ship will be fixed by an enemy. You will find detailed information on the implementation of EMCON and its degree of adjustment in *Electronic*

*Warfare Coordination,* NWP 3-51.1 (formerly NWP 10-1-40).

## SECURITY AREAS

Different spaces aboard ship and different areas within a shore activity usually have varying degrees of security importance. The degree of security of each area depends upon its purpose and the nature of the work, information, equipment, or materials concerned. Access to security areas must be controlled in a manner consistent with the security level.

## SANITIZING SITE AND EQUIPMENT

Sanitizing an area or equipment is done to make it acceptable for access by personnel who are not cleared. This is used to prevent unauthorized persons from gaining access that would allow them to identify the purpose or nature of your work, information, equipment and materials concerned.

To meet this situation, each command should apply differing protective measures commensurate with the degree of security importance. Persons who have not been cleared for access to the information contained within the area, with appropriate approval, may be admitted into an area, but they must be controlled by an escort at all times. Follow guidelines set forth in the *Security Manual* and local standard operating procedures.

A few of the basic requirements are listed below.

- Remove, turn over, or place in drawers any classified material that may be out on desks.
- Replace any keying material in the safe and lock.
- Cover any status boards showing conditions of equipment, frequencies, systems, and so forth.
- Cover all frequencies dialed into equipment.
- Cover monitors or turn off monitor screens if possible.
- Do not conduct any work-related discussions.

At no time will the escort leave someone unattended. The watch section or day working staff maybe required to support the escort in cases where work is being conducted by numerous uncleared personnel in more than one area.

## RESTRICTED AREAS

Designating security spaces as restricted areas provides an effective and efficient means for a command to restrict access and control movement. In restricted areas, only those personnel whose duties actually require access and who have been granted appropriate security clearance are allowed freedom of movement within the area.

Persons who have not been cleared for access to the information contained within the area may, with appropriate approval, be admitted into the area. While in these spaces, however, uncleared persons must be escorted, or other security procedures implemented to prevent any unauthorized disclosure of classified information.

All designated restricted areas must have warning signs posted at all entrances and exits. These areas must have clearly defined perimeters and, if appropriate, Restricted Area warning signs posted on fences and barriers.

### Access to Spaces

The commanding officer or the officer in charge over security spaces is responsible for controlling access to these areas. Procedures should limit access to security spaces only to those persons who have a need to know. No one has a right to have access to classified information or spaces based solely on clearance, rank, or position.

Each command establishes a pass or badge identification system to restrict access and to help control movement. Control of movement within the area is normally accomplished by requiring the display or presentation of the pass or badge for that particular area.

### Access List

Admission of visitors to communications spaces is a topic of major concern to radiomen since access to communications spaces under operating conditions usually permits viewing of classified traffic and equipment. A security badge does not automatically mean that visitors have a “need to know” or that they should be granted access. Admission to communications spaces is granted only to personnel whose names, rates/ranks, and clearance level appear on the official access list.

Access lists, which must be signed and approved by the commanding officer, should be posted at each entrance to a communications space. Admission of persons other than those on the access list is subject to the specific approval of the commanding officer or his or her designated representative.

Personnel not on the access list nor specifically granted permission by the commanding officer for entry must be escorted or supervised at all times while in communications spaces.

### Communications Center Visitors Log

A communications center visitors log (or register) is used to record the arrival and departure of authorized personnel whose names do not appear on the access list. *Fleet Communications* (U), NTP 4, recommends the following column headings for visitors logs:

- Date;
- Visitor's printed name;
- Organization the visitor is representing;
- Purpose of visit;
- Visitor's signature;
- Officer authorizing access to restricted area(s);
- Escort's name;
- Time in; and
- Time out.

### Access to Classified NATO Messages

Only those personnel who hold a security clearance equal to or greater than the clearance required for U.S. material may have access to NATO messages. NATO messages and documents belong to NATO and must not be passed outside the NATO organization. *NATO Security Procedures (U)*, OPNAVINST C5510.101, is the authority for the proper handling, storage, accounting, classification, and clearances of NATO material.

The final responsibility for determining whether a person is granted access to a security area rests upon the individual who has the authorized possession, knowledge, or control of the information involved and not upon the prospective recipient. No number of written rules or governing statutes can replace individual initiative and common sense. As we mentioned earlier, no one has a right to access based solely upon security clearance, rank, or position.

## STORAGE OF CLASSIFIED MATERIAL

All classified matter not in actual use must be stored in a manner that will guarantee its protection. The degree of protection necessary depends on the classification category, quantity, and scope of the material involved. Normally, the type and extent of physical protection required are determined before an activity begins its day-to-day or watch-to-watch routine.

It is very likely that an appropriate physical security program is already in effect when you report aboard. Details concerning physical security standards and requirements for classified information are contained in the *Security Manual.*

### Unattended Containers

If you find an open and unattended container or cabinet containing classified matter, you should report it to the senior duty officer. Do not touch the container or contents, but guard them until the duty officer arrives. The duty officer then assumes responsibility for such further actions as locking the security container, recalling the responsible person or persons, and reporting the security violation to the commanding officer. The custodian must conduct an immediate inventory of the contents of the security container and report any loss to the commanding officer.

### Combinations

Combinations to security containers containing classified material are made available only to those persons whose duties require access to them. The combinations of security containers containing classified information must be changed at least every 2 years, unless more frequent change is dictated by the type of material stored within. Combinations must also be changed under the following circumstances:

- When an individual knowing the combination no longer requires access;
- When the combination has been subject to possible compromise or the security container has been discovered unlocked and unattended; and
- When the container is taken out of service.

The combination of a security container used for the storage of classified material is assigned a security classification equal to the highest category of classified material authorized to be stored in the container. Records of combinations are sealed in an envelope (Standard Form 700) and kept on file in a central location designated by the commanding officer.

### Cipher Locks

Cipher locks and safe combinations are handled in accordance with guidelines found in the *Security Manual*. With the addition of electrically actuated locks (that is, cipher and magnetic strip card locks), this type of lock still does not afford the degree of protection required for classified information. They may NOT be used as the primary means to safeguard classified material. Cipher or magnetic strip card locks are normally used for access to an area only.

## GENERAL MARKING REQUIREMENTS

Classified documents and material must be clearly and conspicuously marked. Special markings, such as LIMDIS and Restricted Data, are normally placed near the classification markings. These markings inform and warn recipients of the classification assigned and indicate the level of protection required. These markings also identify the information that must be withheld from unauthorized persons.

Top Secret, Secret, and Confidential classification markings must be stamped, printed, or written in capital letters larger than those used in the text of the document. These security markings should be red in color, when practicable, and be placed at the top and bottom center of each page.

All reproductions or copies of classified materials, regardless of form, must bear clearly legible security classification markings and notations in the same manner as on the copied or reproduced material. Copying equipment does not always clearly reproduce all colors of ink or marginal images. If the reproduction process does not clearly reproduce the security markings appearing on the original copy, all copies must be marked in the same positions and size as on the original.

Paragraph markings are required for classified documents. The appropriate security markings are placed at the beginning of the classified paragraph. The symbols used to indicate paragraph classification are (TS) for Top Secret,(S) for Secret, (C)for Confidential, and (U) for Unclassified.

It is not uncommon to see foreign-originated classified information in U.S. messages and documents. Paragraphs that contain foreign-originated classified information must be properly marked; for example, "U.K.(C)" or "NATO(S)."

At the beginning of Restricted Data and Formerly Restricted Data paragraphs, use the appropriate classification symbol with the abbreviation "RD" or "FRD," such as "(S-RD)," "(C-FRD)."

Titles and subjects are classified according to their content, regardless of the overall classification of the document. Normally, the symbols indicating the classification assigned to a title or subject are placed in parentheses immediately following the item, as in the following example:

**Subj: BASIC OPERATIONAL COMMUNICATIONS DOCTRINE (U)**

## SPECIAL-HANDLING MARKINGS

In addition to security classification categories, other markings also appear on some documents and messages. Among these markings are such designations as Restricted Data (RD), Formerly Restricted Data (FRD), LIMDIS, FOUO, EFTO, SPECAT, PERSONAL FOR, NATO RESTRICTED, and ALLIED RESTRICTED.

### Restricted Data and Formerly Restricted Data

The marking "Restricted Data" (RD) is applied to all data concerned with the design, manufacture, or use of nuclear weapons. Also included in this category is the special nuclear material used in energy production.

The marking "Formerly Restricted Data" (FRD) pertains to defense information that has been removed from the RD category but must still be safeguarded as classified defense information. FRD material cannot be released to foreign nationals except under specific international agreement.

### LIMDIS (Limited Distribution)

The LIMDIS designator is applied only to classified messages which, because of the subject matter, require limited distribution within the addressed activity.

**For Official Use Only (FOUO)**

FOUO is the designation used on official information not requiring a security classification but which must be withheld and protected from public release. Unclassified messages containing FOUO information must have the abbreviation "FOUO" after the designation "UNCLAS."

**Encrypt for Transmission Only (EFTO)**

Certain categories of unclassified messages maybe identified as having potential value if subject to analysis, but do not meet the criteria for security classification. The special designation "EFTO" was established to protect these unclassified messages during electrical transmission.

EFTO is not required on unclassified messages addressed exclusively among Navy, Marine Corps, and Coast Guard commands. EFTO is authorized for use within the Department of Defense, including the National Security Agency. However, EFTO is required on FOUO messages addressed to DOD activities outside the continental United States. Bear in mind, however, that just because information is FOUO, it is not automatically EFTO, and vice versa.

As we mentioned earlier, EFTO is a transmission marking for unclassified messages. FOUO markings, however, define a certain category of information requiring special handling. Neither FOUO nor EFTO markings are security classifications; both are special-handling designations. You can find detailed information on EFTO and FOUO markings in *Basic Operational Communications Doctrine (U)*, NWP 4.

**SPECAT**

The SPECAT marking means special category. SPECAT messages are classified messages identified with a special project or subject. SPECAT messages require special-handling procedures in addition to the handling procedures for the security classification of the message. There are four SPECAT categories:

- SPECAT;
- SPECAT EXCLUSIVE FOR (SEF);
- SPECAT Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI); and
- PSEUDO-SPECAT.

SPECAT and SPECAT EXCLUSIVE FOR messages must be at least Confidential. SPECAT SIOP-ESI messages are always Top Secret. PSEUDO-SPECAT messages are normally unclassified messages that require limited distribution. Examples of PSEUDO-SPECAT messages include AMCROSS messages, urinalysis test results, and HIV test results.

SPECAT messages are handled only by those personnel who are authorized by the commanding officer in writing to view them. The types of information assigned SPECAT and handling procedures can be found in NWP 4 and in *Fleet Communications (U)*, NWP 4, respectively.

**PERSONAL FOR**

PERSONAL FOR is the marking applied when message distribution must be limited to the named recipient. Only flag officers, officers in a command status, or their designated representatives may originate PERSONAL FOR messages.

**NATO RESTRICTED**

The United States does not have a security classification equivalent to NATO RESTRICTED. NATO messages classified as restricted must be safeguarded in a manner similar to that for FOUO messages. Messages originated by NATO must be handled in accordance with *NATO Security Procedures (U)*, OPNAVINST C5510.101.

**ALLIED RESTRICTED**

The United States does not have a security classification equivalent to ALLIED RESTRICTED. However, these messages must be handled in the same manner as Confidential messages. U.S.-originated messages containing ALLIED RESTRICTED information are marked as "Confidential" immediately following the security classification.

The *Security Manual* contains complete information on paragraph, subparagraph, and document markings.

## HANDLING AND STORAGE OF CLASSIFIED MATERIAL

Classified messages must be provided accounting and control procedures that correspond to their assigned classification. Accounting and control of classified messages serve the following functions:

- Limit dissemination;
- Prevent unnecessary reproduction; and
- Determine the office or person normally responsible for the security of the material.

With Top Secret messages, it is also important to keep a current record of who has the information and who has seen it.

Since distinctions are made among the three levels of classification, distinctions are also made in the degree of accountability and control. Within each command, specific control and accountability procedures are established to ensure that classified material is properly controlled and that access is limited only to cleared personnel.

## SECURITY PERSONNEL

To control classified information with maximum efficiency, the commanding officer designates a security manager, usually an officer. The security manager is responsible for the command's overall security program, which includes the security of classified information, personnel security, and the command's security education program.

In addition, the commanding officer usually appoints a Top Secret Control Officer (TSCO). The TSCO is responsible for the receipt, custody, accounting, and disposition of Top Secret material in the command. The TSCO is normally subordinate to the security manager. If a separate person is not designated as the TSCO, the security manager maybe designated as TSCO. The duties of the security manager and the TSCO are outlined in the *Security Manual.*

Besides the security manager and the TSCO, every command involved in processing data in an automated system must designate an Information System Security Officer (ISSO). The ISSO is responsible to the security manager for the protection of classified information processed in the automated system.

### Custody of Classified Material

An individual who has possession of or is charged with the responsibility for safeguarding and accounting for classified material or information is the "custodian" of that material or information. As a Radioman, you are constantly in possession of classified material, including messages, publications, and equipment. Therefore, you are a custodian of classified material as long as the material is in your possession.

As custodian of classified material, you are responsible for protecting and accounting for the material at all times. You must ensure that the material is protected from disclosure to uncleared personnel, such as a visitor being escorted through your working spaces. If working outside of normal communication spaces, you must ensure that classified material is locked in an approved security container when the material is not in use or under direct supervision.

**CARE DURING WORKING HOURS.—** Every Radioman must take the necessary precautions to prevent access to classified information by unauthorized persons. These precautions include:

- When removed from storage for working purposes, classified documents must be kept under constant surveillance or face down or covered when not in use.
- Preliminary drafts, carbon sheets, plates, stencils, notes, work sheets, and all similar items containing classified information require special precautions. They must be either destroyed immediately after they have served their purpose or given the same classification and safeguarded in the same manner as the classified material produced from them.
- Typewriter ribbons used in typing classified material must be protected in the same manner as the highest level of classification for which they have been used. Fabric typewriter ribbons may be considered as unclassified when both the upper and lower sections have been recycled through the machine five times in the course of regular typing. Those ribbons that are classified must be destroyed as classified waste.

**CARE AFTER WORKING HOURS.—** At the close of each watch or working day, all classified material that is passed from watch to watch must be properly inventoried. Custody is then transferred to the relieving watch supervisor. All other classified material must be locked in an approved security container. A system of security checks at the close of each working day is the best method to ensure that all classified material held is properly protected. Whether your watch section is being relieved by the oncoming watch or you are securing an office space, you should make an inspection to ensure as a minimum that:

- All classified material is properly stored.
- Burn bags are properly stored or destroyed.

- Wastebaskets do not contain classified material.
- Classified notes, carbon paper, carbon and plastic typewriter ribbons, rough drafts, and similar papers have been properly stored or destroyed. As a matter of routine, such items should be placed in burn bags immediately after they have served their purpose.
- When classified material is secured in security containers, the dial of combination locks should be rotated at least four complete turns in the same direction.

## CLASSIFIED MATERIAL (SPECAT/TS AND ABOVE)

Classified material excludes communications security (COMSEC) material, which is handled by CMS 1 procedures. Further in-depth information on classified material can be found in the *Security Manual* and in NTP 4.

1. Receive:

The Top Secret Control Officer (TSCO) is responsible for receiving, maintaining "cradle to grave" accountability registers for, distributing and destroying Top Secret, SPECAT/TS, and above documents.

All Top Secret, SPECAT/TS, and above material received or originated by a command, which the TSCO is responsible for, is entered into the command's accountability log.

Top Secret, SPECAT/TS, and above message traffic, handled by naval communication stations for relay or broadcast delivery only, or received by an afloat command via the fleet broadcast but not addressed to that command will be accounted for and destroyed in accordance with NTP 4.

Top Secret, SPECAT/TS, and above messages addressed to the command are:

- Logged into the cryptocenter log.
- Master copy is placed in the cryptocenter file, and fillers are placed in the appropriate files.
- One copy is given to the TSCO for entry into the command's controlled distribution register.

Top Secret, SPECAT/TS, and above messages received by an afloat command but NOT addressed to the command via the broadcast:

- Only the text will be removed from the monitor roll.
- The message will be destroyed, and the monitor roll will be initialed by two witnessing officials.
- The broadcast serial number checkoff sheet will also be initialed by two witnessing officials.

2. Destroy:

Top Secret, SPECAT/TS, and above material will be destroyed by two witnessing officials. Persons performing any destruction must have a clearance level equal to or higher than the material being destroyed. The destruction of Top Secret, SPECAT/TS, and above material must be recorded. Destruction may be recorded on OPNAV form 5511/12 (figure 5-1), or any other record which includes complete identification of the material, number of copies destroyed, date of destruction, and personnel completing destruction. The two witnessing officials responsible for the destruction must sign the record of destruction. The records of the destruction are retained for 2 years.

3. Verify destruction:

The destruction of Top Secret, SPECAT/TS, and above material must be verified by both witnesses signing the destruction sheet and either turning it over to the TSCO or placing it in the cryptocenter master file until it is superseded, usually within 2 years.

## HANDLING TOP SECRET MATERIAL

Although administrative records are maintained for each classification category, the strictest control system is required for Top Secret material.

Except for publications containing a distribution list by copy number, all Top Secret documents and each item of Top Secret equipment must be serially numbered at the time of origination. Also, each document must be marked to indicate its copy number (for example, Copy No. ___ of ___ Copies).

Each page of a Top Secret document not containing a list of effective pages (LOEP) must be individually numbered (for example, Page ___ of ___ pages). Top Secret documents are required to have a list of effective pages and a page-check page. Top Secret documents may be reproduced only with the permission of the originator or higher authority.

| CLASSIFIED MATERIAL DESTRUCTION REPORT<br>OPNAV 5511/12 (REV. 3-75) S/N 0107-LF-055-1160<br>TO: Commanding Officer, USS NEVERSAIL | CLASSIFICATION *(Indicate when title or other identification is classified)*<br>UNCLASSIFIED |
|---|---|

FROM *(Name and address of activity)*
Top Secret Control Officer

The classified material described below has been destroyed in accordance with regulations established by the Department of the Navy Information Security Program Regulation; OPNAV INSTRUCTION 5510.1G.

The purpose of this form is to provide activities with a record of destruction of classified material. Also, copies may be utilized for reports to activities originating material, where such reports are necessary.

DESCRIPTION OF MATERIAL

| SERIAL/DTG | ORIGINATOR | DATE | COPY NO. | LOG/ ROUTE SHEET NO. | ENCLOSURES (IDENT. & NO.) | TOTAL NO. PAGES |
|---|---|---|---|---|---|---|
| 00052 | CINCPACFLT letter | (Date) | 1 | 4 | | 4 |

| OFFICER OR INDIVIDUAL AUTHORIZING DESTRUCTION *(Signature, Rank/Rate/Grade)* | DATE OF DESTRUCTION<br>(Date) |
|---|---|
| WITNESSING OFFICIAL *(Signature, Rank/Rate/Grade)*<br>John Doe | WITNESSING OFFICIAL *(Signature, Rank/Rate/Grade)*<br>Jane Smith |

Figure 5-1.—Classified Material Destruction Report.

A continuous chain of receipts for Top Secret material must be maintained. Moreover, a Record of Disclosure, OPNAV form 5511/13, for Top Secret material is attached to each document that circulates within a command or activity. Each person having knowledge of the contents of a Top Secret document must sign the attached Record of Disclosure. Top Secret messages, documents, and publications must be stored in a security container separate from those classified Secret and below.

**HANDLING SECRET MATERIAL**

Every command is required to establish administrative procedures for recording all Secret material originated and received. These administrative procedures, as a minimum, must include a system of accountability for Secret matter distributed or routed within the command, such as a communications log. Accounting of Secret material may or may not be centralized.

Unlike Top Secret material, Secret material does not require signed receipts distributed or routed within the command. However, it is extremely important that you ensure that the person who is receiving Secret messages or material is properly cleared, and his or her name appears on an access list released by the commanding officer.

**HANDLING CONFIDENTIAL MATERIAL**

Procedures for handling Confidential material are less stringent than those for Secret. There is no requirement to maintain records of receipt, distribution, or disposition of Confidential material. However, Confidential material must still be protected from unauthorized disclosure by access control and compliance with regulations on marking, storage, transmission, and destruction.

**HANDLING CLASSIFIED AIS MATERIAL**

Classified AIS storage media and output must be controlled and safeguarded in accordance with its security classification. Specific procedures on security requirements for handling and storing AIS material are found in the *Department of the Navy Automatic Data Processing Security Program*, OPNAVINST 5239.1.

## CLEARING MEDIA AND HARDWARE

Declassifying AIS media is a procedure to erase totally all classified information stored in the media. The clearing of AIS media is used to erase classified information that lacks the totality and finality of declassifying. There are distinct and specific techniques to clear media and hardware; a sampling follows:

- Magnetic tapes: Overwrite one item with any one character or perform degaussing.
- Magnetic media used to store analog, video, or other nondigital information: Overwrite using analog signals instead of digital.
- Internal memory, buffers, registers, or similar storage areas: Use hardware clear switch, power on reset cycle or a program designed to overwrite the storage area.
- Cathode-ray tubes (CRTs): Ensure that there is no burned-in classified information by inspecting the screen surface.

## DESTRUCTION OF CLASSIFIED MATERIAL

Classified material that is no longer required should not be allowed to accumulate. Destruction of superseded and obsolete classified materials that have served their purpose is termed "routine destruction."

**ROUTINE DESTRUCTION**

There are specific directives that authorize the routine destruction of publications, message files, and cryptomaterials. As a Radioman, you should carefully study these directives so that you may properly comply with them. Additionally, the letter of promulgation of publications often sets forth disposition instructions about destruction requirements for that publication. Other materials, such as classified rough drafts, worksheets, and similar items, are periodically destroyed to prevent their accumulation.

Top Secret, Secret, and Confidential material may be destroyed by burning, pulping, pulverizing, or shredding. Destruction must be complete and reconstruction of material impossible. The most efficient method of destroying combustible material is by burning.

**DESTRUCTION PROCEDURES AND REPORTS**

Top Secret material will be destroyed by two witnessing officials. Persons performing any destruction must have a clearance level equal to or

higher than the material being destroyed. Destruction will be recorded on a record that provides for complete identification of the material being destroyed. Destruction records must include number of copies destroyed, date of destruction, and personnel completing destruction. These records are maintained for 2 years.

Secret messages must be destroyed following the two-person rule, without a record of destruction. Alternatively, one person may destroy Secret messages if a record of destruction is made. The commanding officer may impose additional controls for Secret messages if warranted and if they reasonably balance security against operational efficiency.

Confidential material and classified waste are destroyed by authorized means. Personnel performing destruction must hold an appropriate clearance and are not required to record destruction.

If the material has been placed in burn bags for central disposal, the destruction record is signed by the witnessing officials at the time the material is placed in the burn bags. Records of destruction must be retained for 2 years.

All burn bags must be given the same protection as the highest classification of material in them until they are destroyed. Since several burn bags may accumulate for burning, it is important to keep an accurate record of the number of bags to be burned. Burn bags must be serially numbered and a record kept of all subsequent handling until destroyed.

### Burning

As a Radioman, you will probably assist in the burning of classified material. Every member of a burn detail must know exactly what is to be burned and should double-check burn material against an inventory list before the material is burned.

To provide for accountability of the burn bags, the supervisor of a burn detail must be sure that the bags are numbered (or counted) before they are removed from the workspaces. The supervisor of a burn detail must have either a log or checkoff list that lists the number of bags to be burned. At the destruction site, each bag is checked off the list as it is destroyed in the presence of the witnessing officials. Witnessing officials are persons performing any destruction. They must have a clearance equal to or higher than the material being destroyed.

To ensure the complete destruction of bound publications, the pages must be torn apart and crumpled before they are placed in bags. All material must be watched until it is completely consumed. The ashes must be broken up and scattered so that no scraps escape destruction.

### Shredding

Crosscut shredding machines are relatively quiet and may be used aboard ships where incinerator facilities are not available. Crosscut shredders are replacing incinerators in many areas where burning is not allowed because of the Clean Air Act. Crosscut shredding machines must reduce classified material to shreds no greater than 3/64 inch wide by 1/2 inch long. Crosscut shredding suffices as complete destruction of classified material, and the residue may be handled as unclassified material with the exception of some COMSEC material. Not all crosscut shredders are suitable for destroying microfiche, so make sure the one you are using has that capability before attempting to shred microfiche.

### Pulverizing and Disintegrating

Pulverizers and disintegrators designed for destroying classified material are usually too noisy and dusty for office use unless installed in a noise- and dust-proof enclosure. Some pulverizers and disintegrators are designed to destroy paper products only. Others are designed to destroy film, typewriter ribbons, photographs, and other material.

### Jettisoning or Sinking

Material to be jettisoned during emergency destruction must be placed in weighted bags. The sea depth should be 1,000 fathoms or more. However, if water depth is less than 1,000 fathoms, the material should still be jettisoned to prevent easy recovery.

## EMERGENCY PLANS

Emergency plans provide for the protection, removal, or destruction of classified material. Commands holding classified material must develop an emergency plan to fit their needs. The primary requirement of an emergency plan is that it adequately provide for the rapid and complete destruction of the classified material. Emergency plans must cover three areas of emergencies:

- Natural disasters, such as hurricanes;
- Civil disturbances, such as rioting; and
- Enemy action.

Emergency plans should provide for the protection of classified material in such a manner as to minimize the risk of loss of life or injury to personnel.

For destruction, the command's emergency plan must do the following:

- Emphasize procedures and methods of destruction, including place and destruction equipment required;
- Clearly identify the exact location of all classified material;
- Prioritize material for destruction; and
- Assign personnel by billet, areas of responsibility for destruction.

**Priorities**

When the emergency plan is implemented, priority of destruction is based on the potential effect on national security should the material fall into hostile hands. COMSEC material is destroyed first. The priorities for emergency destruction are as follows:

- **FIRST PRIORITY—** Top Secret COMSEC material and classified components of equipment and all other Top Secret material;
- **SECOND PRIORITY—** Secret COMSEC material and all other Secret material;
- **THIRD PRIORITY—** Confidential COMSEC material and all other Confidential material.

After you have destroyed the classified for which you are responsible, you should destroy any unclassified equipment that could be of use to an enemy. You should also destroy pertinent technical, descriptive, and operating instructions.

**FIRE PLANS**

In addition to an emergency plan, a plan of action in the event of fire is also required. As with an emergency plan, it is important that all comunications personnel familiarize themselves with their command fire plan. Normally, the fire plan provides for the following:

- Local fire-fighting apparatus and personnel to operate the equipment;
- Evacuation of the area, including a decision whether to store classified material or remove it from the area; and
- Admitting outside fire fighters into the area.

**PRECAUTIONARY ACTIONS**

Precautionary destruction reduces the amount of classified material on hand in case emergency destruction later becomes necessary. Destruction priorities remain the same during precautionary destruction. However, when precautionary destruction is held, material essential to communications must not be destroyed. For example, communications operating procedures and publications that are to become effective in the near future would not be destroyed. Communications operating procedures that are already effective, necessary, and being used would also not be destroyed.

The following actions should be taken daily:

- All superseded material should be destroyed in accordance with its prescribed time frame.
- Unneeded material should be returned to the issuing agencies.
- Material should be stored in such a way as to make it readily accessible for removal during destruction.

Contrary to widespread opinion, there is no security policy requiring destruction of unclassified messages. However, some message centers with high volumes of classified and unclassified message traffic may find it more efficient to destroy all messages and intermingled files as though they were classified. Under some circumstances, units operating in foreign ports or waters and commands situated in foreign countries may take additional precautions in disposing of unclassified material.

## SUMMARY

This chapter has discussed general security considerations to provide you with a working knowledge of this important aspect of your job. As a Radioman, you have a two-fold job concerning security. The first, of course, is to properly perform your duties within general security guidelines. Security guidelines pertain to everyone in every official capacity. Second, you must also perform your duties in such a manner as to protect the integrity and overall value of secure communications.

Security should be second nature insofar as the practice of personal habits is concerned. However, second nature does not mean "without thinking." It behooves all of us to take security seriously and practice sound security habits in the interests of naval operations and our overall national security.

Security precautions mentioned in this chapter do not guarantee complete protection nor do they attempt to meet every conceivable situation. Anyone who adopts a commonsense outlook can, however, solve most security problems and gain a knowledge of basic security regulations.

## APPENDIX I

# GLOSSARY

**A**

**ADDRESS GROUPS—** Four-letter groups assigned to represent a command, activity, or unit; used in the same manner as a call sign.

**AIS FACILITY-RELATED INFORMATION—** Workload, anticipated resource changes, number of operators available, the system capabilities, etc.

**B**

**BACKLOG—** The work waiting to be run (processed) on a computer.

**BATCH PROCESSING—** A method of processing in which similar items are grouped together and processed all at one time.

**BOOK MESSAGE—** A message for two or more addressees in which the drafter considers it unnecessary that each addressee be informed of the other(s).

**C**

**CMS ALTERNATE CUSTODIAN—** Responsible to the CMS custodian and commanding officer for the CMS account; is held accountable on the same level as the custodian.

**CMS CUSTODIAN—** Responsible to the commanding officer for the correct accountability and maintenance of the CMS account.

**CMS LOCAL HOLDER—** A command or activity that receives COMSEC material support from a CMS account command.

**CMS USER—** An individual CMS user that requires COMSEC material to accomplish an assigned duty, advancement study, or training purpose.

**COMMUNICATIONS CENTER SUPERVISOR—** Responsible for message processing, circuit operations, and supervision of personnel; responsible to the SWS, when assigned.

**COMMSHIFT—** A message sent to a NCTAMS to move its guard from one broadcast or servicing communications center to another.

**COMMSPOT—** A report to advise of any situation that might cause significant disruption to tactical communications.

**COMNAVCOMTELCOM** (COMMANDER, NAVAL COMPUTER AND TELECOMMUNICATIONSCOMMAND)— Headquarters for all naval shore-based communications.

**CONTINGENCY PLANS—** Backup plans for the continuation of an activity's mission during abnormal operating conditions.

**CWO** (COMMUNICATIONS WATCH OFFICER)— Responsible for the efficient running of the watch, including equipment and personnel; responsible to the communications officer.

**D**

**DRAFTER—** The person who actually composes a message for transmission.

**DTG** (DATE-TIME GROUP)— A method of assigning a date and time to message traffic consisting of six digits, two each to represent date, hour, and minutes; begins at the start of each new day at 0001Z.

**E**

**EA** (ELECTRONIC ATTACK)— Involves actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum. EA replaces electronic countermeasures (ECM).

**ELECTROMAGNETIC SPECTRUM–** The natural vibrations that occur when a force is applied to a substance. These vibrations occur with various speeds and intensities. The speed at which they occur is called frequency, and the distance between each vibration is called wavelength.

**EMERGENCY PLAN—** Provides for the protection, removal, or destruction of classified material.

**EP** (ELECTRONIC PROTECTION)— Involves actions taken to ensure friendly effective use of the electromagnetic spectrum despite an enemy's use of electronic warfare. EP replaces electronic counter-countermeasures (ECCM).

**EXTRACTS—** Portions of naval warfare publications that are extracted/reproduced for use in training or operations. All extracts must be properly marked with security classification and safeguarded.

**F**

**FLASH PRECEDENCE—** Identified by the precedence prosign "Z." Category reserved for initial enemy contact reports or operational combat messages of extreme urgency. Brevity is mandatory. Speed of service objective is not fixed. Handled as fast as humanly possible with an objective of less than 10 minutes.

**FRD** (FORMERLY RESTRICTED DATA)– Pertains to defense information that has been removed from the Restricted Data category but is still safeguarded as classified defense information.

**G**

**GENERAL MESSAGE—** A message with wide, predetermined and standard distribution.

**I**

**IFF** (IDENTIFICATION FRIEND OR FOE)— A system using electromagnetic transmissions to which equipment carried by friendly forces automatically responds to distinguish themselves from enemy forces.

**IMMEDIATE PRECEDENCE—** Identified by the precedence prosign "O." Delivery time reserved for very urgent messages relating to situations that gravely affect the security of national/allied forces. Examples of use: amplifying report of initial enemy contact or unusual major movements of military forces. Speed of service objective is 30 minutes to 1 hour.

**INMARSAT** (INTERNATIONAL MARITIME SATELLITE COMMUNICATIONS)— A satellite system that interfaces naval communications for the DON and commercial telecommunications authorized by law.

**I/O CONTROL CLERK—** The person responsible for the quality and control of data processing input and output media and products.

**J**

**JETTISONING—** A type of destruction that is completed by throwing material overboard at sea at a depth of at least 1,000 fathoms or more; also known as Sinking.

**JOB DEPENDENCY—** When a job requires the output from another job, it is said to be dependent on another job.

**JOB-RELATED INFORMATION—** Information about the resources, media, and time needed for a particular job.

**JULIAN DATE—** Consists of seven digits; the first three digits represent the date, and the last four digits represent the hour and minutes; begins on the first day of the calendar year.

**M**

**MARS** (MILITARY AFFILIATE RADIO SYSTEM)— Provides auxiliary communications to military, civil, and/or disaster officials during periods of emergency. Users are licensed by the Federal Communications Commission (FCC).

**MULTIPLE-ADDRESS MESSAGE—** A message with two or more addressees.

**MULTIPROCESSING—** A computer processing mode that provides for simultaneous processing of two or more programs or routines by use of multiple CPU's.

**MULTIPROGRAMMING—** A computer processing mode that provides for overlapping or interleaving the execution of two or more programs at the same time by a single processor.

**N**

**NETWORKING—** A processing mode that allows separate computers, joined by transmission lines, to share a group of common peripherals.

**NWPL CLERK—** Usually assigned by the NWPL custodian and is responsible for the upkeep and maintenance of the NWPL.

**NWPL CUSTODIAN—** Is responsible for managing the NWPL, usually assigned to an officer or senior petty officer as a collateral duty.

**O**

**ONLINE—** A method of data processing that allows users the ability to interact with the computer.

**ORIGINATOR—** The authority in whose name a message is sent.

**P**

**PERSONAL FOR–** Messages distributed to a single recipient. Only flag officers, officers in a command status, or their designated representative may originate PERSONAL FOR messages.

**PLANNING PHASE—** The initial scheduling phase in which information is gathered from the users.

**POSTCOMPUTER PROCESSING—** Ensuring output products are complete, accurate, and delivered to the user.

**PRECAUTIONARY ACTIONS OR PRECAUTIONARY DESTRUCTION—** An action to remove or reduce the amount of classified material on hand in case emergency destruction becomes necessary at a later time.

**PRECEDENCE—** A delivery time assigned to a message according to the urgency of that message, based solely on writer-to-reader time.

**PRECOMPUTER PROCESSING—** Ensuring all inputs are received on time.

**PRIORITY PRECEDENCE—** Identified by the precedence prosign "P." Delivery time reserved to message for essential information for the conduct of operations in progress. Examples of use: situation reports on position of front where attack is imminent, orders to aircraft formation or units to coincide with ground or naval operations. Speed of service objective is 1 to 6 hours.

**R**

**RD** (RESTRICTED DATA)— Pertains to all data concerned with the design, manufacture, or use of nuclear weapons or special nuclear material used in energy production.

**REAL-TIME PROCESSING—** A computer processing method in which data about a particular event is entered directly into the computer as the event occurs and is immediately processed so it can influence future processing.

**RELEASER—** A properly designated individual authorized to release messages for transmission in the name of the command or activity.

**RESTRICTED AREA—** Designated spaces that restrict access and control movement within.

**ROUTINE PRECEDENCE—** Identified by the precedence prosign "R." Delivery time assigned to be used for all types of message which does not justify a higher precedence. Examples of use: administrative, logistics, or personnel matters. Speed of service objective is 3 hours or start of business the following day.

**S**

**SANITIZING—** Makes an area or equipment acceptable for access by personnel who are not cleared.

**SCHEDULER—** The person responsible for preparing, distributing, and maintaining production schedules.

**SCHEDULING—** The interface between the user, I/O control, and computer operations.

**SHREDDING—** A type of destruction that involves using a cross-cut shredding machine. Residue must be reduced to shreds no greater than 3/64 inch wide by 1/2 inch long.

**SINGLE-ADDRESS MESSAGE—** A message with only one addressee.

**SPECIAL-HANDLING MARKINGS—** Additional markings or designations on some messages that alert the user or communications center that the message requires special attention in handling. Some of these include Caveat, Restricted Data (RD), Formerly Restricted Data (FRD), FOUO, EFTO, SPECAT, and PERSONAL FOR.

**SWS** (SENIOR WATCH SUPERVISOR)— When assigned, the senior enlisted person on watch responsible for handling all communications matters; responsible to the CWO.

**T**

**TECH CONTROL SUPERVISOR—** Responsible for establishing and maintaining required circuits, including initiating actions to restore or bypass failed equipment, quality monitoring, supervising assigned personnel, and controlling procedures for all systems; responsible to the CWO.

**TELEPROCESSING—** A method of data processing in which communications devices are used.

**TERMINATION REQUEST MESSAGE—** A message sent to request establishment of circuits with a NCTAMS or NAVCOMTELSTA on a limited or fill-time basis.

**TIME SHARING—** A processing mode in which users share computer system resources through online terminals.

**TSCO** (TOP SECRET CONTROL OFFICER)— An officer, senior noncommissioned officer (E-7, E-8, or E-9) or a civilian employee, (GS-7 or above) who is responsible for the receipt, custody, accounting, and disposition of Top Secret material within the command.

**TSO** (TELECOMMUNICATIONS SERVICE ORDER)— Used to authorize the start, change, or discontinue circuits, trunks, links, or systems.

**TSR** (TELECOMMUNICATIONS SERVICE REQUEST)—Initiates additions, deletions, or changes from the originating command to existing Defense Communications System (DCS) circuits.

**TVA** (TEMPEST VULNERABILITY ASSESSMENT)— The vulnerability of a ship, aircraft, shore station transportable equipment, or a contractor facility to susceptibility, environment, and threat.

**TVAR** (TEMPEST VULNERABILITY ASSESSMENT REQUEST)— A request submitted prior to processing classified data to the Naval Criminal Investigation Service.

**Y**

**YANKEE PRECEDENCE—** This category is in addition to the four major precedences categories; it is an EMERGENCY COMMAND PRECEDENCE (ECP). It is identified by the precedence prosign "Y" and limited to designated emergency action command and control messages. Speed of service objective is not fixed. Handled as fast as humanly possible with an objective of less than 10 minutes.

## APPENDIX II

# GLOSSARY OF ACRONYMS AND ABBREVIATIONS

**A**

**ACP—** Allied communications publication.
**AIG—** Address indicating group.
**AIS—** Automated information system.
**ALCOM—** All commands.
**ALNAV—** All Navy.
**AMCROSS—** American Red Cross.
**ATP–** Allied tactical publication.
**AUTODIN—** Automatic Digital Network.
**AXP—** Allied exercise publication.

**B**

**BKS—** Broadcast keying station.
**BSR—** Broadcast screening request.

**C**

**CE—** Compromising emanations.
**CIB—** Communications Information Bulletin.
**CIC—** (1) Content Indicator Code (2) Combat Information Center.
**CINCLANTFLT—** Commander in Chief, Atlantic Fleet.
**CINCPACFLT—** Commander in Chief, Pacific Fleet.
**CMS—** Communications Security Material System.
**CNO—** Chief of Naval Operations.
**COMMAREA—** Communications area.
**COMMO—** Communications Officer.
**COMMSHIFT—** Communications shift.
**COMMSPOT—** Communications spot report.
**COMNAVCOMTELCOM—** Commander, Naval Computer and Telecommunications Command.
**COMNAVSECGRU—** Commander, Naval Security Group.
**COMNAVSURFLANT—** Commander, Naval Surface Forces Atlantic.
**COMSEC—** Communications security.
**COSIR—** Cite our service in return.
**CP—** Change proposal.
**CRT—** Cathode-ray tube.
**CWO—** Communications Watch Officer.

**D**

**DCS–** (1) Defense Courier Service (2) Defense Communications Service.
**DCMS—** Director, Communications Security Material System.
**DESRON—** Destroyer squadron.
**DISA—** Director, Information Security Agency.
**DON—** Department of the Navy.
**DODCAF—** Department of Defense Central Adjudication Facility.
**DSCS—** Director, Satellite Communications System.
**DSR—** Data speed reader.
**DTG—** Date-time group.

**E**

**EA—** Electronic attack (replaces electronic countermeasures (ECM)).
**EAM—** Emergency Action Message.
**EASTPAC—** Eastern Pacific.
**ECP—** Emergency command precedence.
**EFTO—** Encrypt for transmission only.
**EMCON—** Emanation control.
**EOJ—** End of job.
**EP—** Electronic protection (replaces electronic counter-countermeasures (ECCM)).

**F**

**FC—** Fixed-cycle.
**FCC—** Federal Communications Commission.
**FIFO—** First-in, first-out.
**FLTCINC—** Fleet Commander in Chief.
**FOTP—** Fleet Operational Telecommunications Program.
**FOUO—** For Official Use Only.
**FRD—** Formerly Restricted Data.
**FTOC—** Fleet Telecommunications Operations Center.
**FTP—** Fleet training publication.
**FXP—** Fleet exercise publication.

**G**

**GENADMIN—** General Administrative.
**GHz—** Gigahertz.
**GMT—** Greenwich Mean Time.

**H**

**HF—** High frequency.
**HW—** Hardware.

**I**

**IDL—** International Date Line.
**IDS—** Intrusion Detection System.
**IFF—** Identification, friend or foe.
**INMARSAT—** International Maritime Satellite System.
**IR—** Information resources.
**ISSM—** Information Systems Security Manager.
**ISSO—** Information Systems Security Officer.
**ITS—** Instrumented TEMPEST Survey.

**J**

**JANAP—** Joint Army-Navy-Air Force Publication.
**JCS—** Joint Chiefs of Staff.

**K**

**kHz—** Kilohertz.

**L**

**LANT—** Atlantic.
**LDMX—** Local Digital Message Exchange.
**LIMDIS—** Limited distribution.
**LMF—** Language and media format.
**LOEP—** List of effective pages.

**M**

**MARS—** Military Affiliate Radio System.
**MED—** Mediterranean.
**MIJI—** Meaconing, Interference, Jamming, and Intrusion.
**MTF—** Message text format.

**N**

**NARDAC—** Naval Regional Data Automation Center.
**NATO—** North Atlantic Treaty Organization.
**MMAREA—** Naval communications area.
**NAVCOMPARS—** Naval Communications Processing and Routing System.
**NAVCOMTELDET—** Naval Computer and Telecommunications Detachment.
**NAVCOMTELCOM—** Naval Computer and Telecommunications Command.
**NAVCONTELSTA—** Naval Computer and Telecommunications Station.
**NAVDAC—** Naval Data Automation Center.
**NAVDAF—** Naval Data Automation Facility.
**NAVELEXSECCEN—** Naval Electronics Security Center.
**NAVEMSCEN—** Naval Electromagnetic Spectrum Center.
**NAVOP—** Naval Operations.
**NAVSECGRUDEPT—** Naval Security Group Department.
**NAVTELCOM—** Naval Telecommunications Command.
**NCS—** (1) Naval Communications Station (2) National Communications System (3) Net Control Station.
**NCTAMS—** Naval Computer and Telecommunications Area Master Station.
**NCTS—** Naval Computer and Telecommunications Station.
**NIF—** Naval Industrial Fund.
**NMC—** Numerical message correction.
**NOTAM—** Notice to airmen.
**NSO—** Network Security Officer.
**NTIA—** National Telecommunications and Information Administration.
**NTP—** Naval telecommunications publication.
**NTS—** Naval Telecommunications System.
**NWPC—** Naval warfare publications custodian.
**NWPL—** Naval Warfare Publications Library.
**NWP—** Naval warfare publication.

**O**

**OPORD—** Operation Order.
**OSRI—** Originating station routing indicator.
**OTAR—** Over-the-air rekey.
**OTAT—** Over-the-air transfer.

**P**

**PCMT—** Personal Computer Message Terminal.
**PC—** Personal computer.
**PLA—** Plain Language Address.

**PQS—** Personnel Qualification Standards.
**PRO FORMA—** Predetermined format.
**PROSIGNS—** Procedural signs.
**PSN—** Processing sequencing number.

**R**

**RADAY—** Radio day.
**RD—** Restricted Data.
**RI—** Routing indicator.
**RMKS—** Remarks.

**S**

**SEF—** SPECAT Exclusive For.
**SIGSEC—** Signal security.
**SIOP-ESI—** Single Integrated Operational Plan-Extremely Sensitive Information.
**SOG—** Special Operating Group.
SOP—Standard operating procedure.
**SPECAT—** Special Category.
**SSN—** Station serial number.
**SUBMISS—** Submarine missing.
**SUBRON—** Submarine squadron.
**SUBSUNK—** Submarine sunk.
**SVC—** Service.
**SWS—** Senior Watch Supervisor.

**T**

**TASO—** Terminal Area Security Officer.
**TCC—** Telecommunications Center.
**TICON—** Tight control.
**TOD—** Time of delivery.
**TOF—** Time of file.
**TOR—** Time of receipt.
**TPI—** Two-person integrity.
**TR—** Trouble report.
**TSC—** Top Secret control officer.
**TSEC—** Telecommunications security.
**TSO—** Telecommunications service order.
**TSR—** Telecommunications service request.
**TVA—** TEMPEST Vulnerability Assessment.
**TVAR—** TEMPEST Vulnerability Assessment Request.

**U**

**UPS—** Uninterrupted power supply.
**US&P—** United States and Possessions.
**USMCEB—** United States Military Communications-Electronics Board.

**V**

**VDT—** Video display terminal.

**W**

**WESTPAC—** Western Pacific.

**Z**

**ZDK—** Send again (“Z” signal).
**ZUI—** Your attention is invited to . . . (“Z” signal).

## APPENDIX III

# REFERENCES USED TO DEVELOP THE TRAMAN


*Allied Call Sign and Address Group System–Instructions and Assignments,* ACP 100(F), Joint Chiefs of Staff, Washington, DC, March 1984.

*Automatic Digital Network (AUTODIN) Operating Procedures,* JANAP 128(J), Joint Chiefs of Staff, Washington, DC, July 1993.

*Bask Operational Communications Doctrine (U),* NWP 4 (Rev. B) (NWP 6-01), Chief of Naval Operations, Washington, DC, September 1989.

*Communication Instructions General (U),* ACP 121(F), Joint Chiefs of Staff, Washington, DC, April 1983.

*Communications Instructions—General,* ACP 121 US SUPP-1(F), Joint Chiefs of Staff, Washington, DC, June 1981.

*Communications Instructions Security (U),* ACP 122, Joint Chiefs of Staff, Washington, DC, 1981.

*Communication Instructions—Operating Signals,* ACP 131(D), Joint Chiefs of Staff, Washington, DC, May 1986.

*Communications Instuctions–Tape Relay Procedures,* ACP 127(G), Joint Chiefs of Staff, Washington, DC, November 1988.

*Communications Instructions–Teletypewriter (Teleprinter) Procedures,* ACP 126(C), Joint Chiefs of Staff, Washington, DC, May 1989.

*Communications Security Material System (CMS) Policy and Procedures Manual,* CMS 1, Department of the Navy, Washington, DC, March 1993.

*Department of the Navy Automated Information Systems (AIS) Security Program,* SECNAVINST 5239.2, Secretary of the Navy, Washington, DC, November 1989.

*Department of the Navy Information and Personnel Security Program Regulation,* OPNAVINST 5510.1H, Chief of Naval Operations, Washington, DC, May 1991.

*Department of the Navy Physical Security and Loss Prevention,* OPNAVINST 5530.14B, Chief of Naval Operations, Washington, DC, December 1988.

*Department of the Navy Privacy Act (PA) Program,* SECNAVINST 5211.5D, Secretary of the Navy, Washington, DC, July 1992.

*Department of the Navy Security Program for Automatic Data Processing Systems*, OPNAVINST 5239.1A, Chief of Naval Operations, Washington, DC, August 1982.

*Fleet Communications (U)*, NTP 4(C), Commander, Naval Telecommunications Command, Washington, DC, June 1988.

*Fleet Telecommunications Procedures for Atlantic and Mediterranean Naval Communications Areas*, NCTAMS LANT/MEDINST C2300.1, Naval Computer and Telecommunications Area Master Station LANT/Naval Computer and Telecommunications Area Master Station MED, September 1993.

*Fleet Telecommunications Procedures for the Pacific and Indian Ocean Naval Communication Areas*, NCTAMSEASTPAC/NCTAMS WESTPACINST C2000.3D, Naval Computer and Telecommunications Area Master Station EASTPAC/Naval Computer and Telecommunications Area WESTPAC, 10 August 1992.

*Guideline for Automatic Data Processing Risk Analysis*, Federal Information Processing Standards (FIPS) Publication 65, Department of Commerce, National Bureau of Standards, Springfield, VA, August 1979.

*Guideline for Evaluation of Techniques for Automated Personal Identification*, Federal Information Processing Standards (FIPS) Publication 48, Department of Commerce, National Bureau of Standards, Springfield, VA, April 1977.

Hussain, Donna, and K. M. Hussain, *Managing Computer Resources*, Second Edition, Richard D. Irwin, Inc., Homewood, IL, 1988.

Local SOP and PQS, Bureau of Naval Personnel (PERS-1043B), Washington, DC.

Local SOP and PQS, Enlisted Program Management Center (EPMAC), New Orleans, LA.

Local SOP and PQS, USS EISENHOWER (CVN-69).

Local SOP and PQS, USS NASSAU (LHA-4).

*Message Address Directory*, Joint Chiefs of Staff, Washington, DC, June 1990.

*Naval Warfare Documentation Guide*, NWP 0 (Rev. P) (NWP 1-01), Chief of Naval Operations, Washington, DC, January 1990.

*Operational Reports*, NWP 10-1-10 (NWP 1-03.1), Chief of Naval Operations, Washington, DC, November 1987.

*Security Requirements for Automated Information Systems (AISs)*, DODD 5200.28, Deputy Security of Defense, Washington, DC, March 1988.

*Telecommunications Users Manual*, NTP 3(1), Commander, Naval Telecommunications Command, Washington, DC, January 1990.

*U.S. Call Sign & Address Group System Instructions & Assignments,* ACP 100 U.S. SUPP-1(N), Joint Chiefs of Staff, Washington, DC, June 1989.

*U.S. Navy Address Indicating Group (AIG) and Collective Address Designator (CAD) Handbook, NTP* 3 SUPP-1(K), Commander, Naval Telecommunications Command, Washington, DC, August 1986.

# INDEX

**N**

*U.S. Government Printing Office: 1998 - 633-154/60099

# RADIOMAN TRAINING SERIES
## MODULE 1 - ADMINISTRATION AND SECURITY

**NAVEDTRA 12845**

Prepared by the Naval Education and Training Professional Development and Technology Center (NETPDTC), Pensacola, Florida

Congratulations! By enrolling in this course, you have demonstrated a desire to improve yourself and the Navy. Remember, however, this self-study course is only one part of the total Navy training program. Practical experience, schools, selected reading, and your desire to succeed are also necessary to successfully round out a fully meaningful training program. You have taken an important step in self-improvement. Keep up the good work.

---

### HOW TO COMPLETE THIS COURSE SUCCESSFULLY

ERRATA: If an errata comes with this course, make all indicated changes or corrections before you start any assignment. Do not change or correct the associated text or assignments in any other way.

TEXTBOOK ASSIGNMENTS : The text pages that you are to study are listed at the beginning of each assignment. Study these pages carefully before attempting to answer the questions in the course. Pay close attention to tables and illustrations because they contain information that will help you understand the text. Read the learning objectives provided at the beginning of each chapter or topic in the text and/or preceding each set of questions. In the course. Learning objectives state what you should be able to do after studying the material. Answering the questions correctly helps you accomplish the objectives.

SELECTING YOUR ANSWERS: After studying the associated text, you should be ready to answer the questions in the assignment. Read each question carefully, then select the BEST answer. Be sure to select your answer from the subject matter in the text. You may refer freely to the text and seek advice and information from others on problems that may arise in the course. However, the answers must be the result of your own work and decisions. You are prohibited from referring to or copying the answers of others and from giving answers to anyone else taking the same course. Failure to follow these rules can result in suspension from the course and disciplinary action.

ANSWER SHEETS: You must use answer sheets designed for this course (NETPMSA Form 1430/5, Stock Ordering Number 0502-LP-216-0100). Use the answer sheets provided by Educational Services Officer (ESO), or you may reproduce the one in the back of this course booklet.

SUBMITTING COMPLETED ANSWER SHEETS: As a minimum, you should complete at least one assignment per month. Failure to meet this requirement could result in disenrollment from the course. As you complete each assignment, submit the completed answer sheet to your ESO for grading. You may submit more than one answer sheet at a time.

GRADING : Your ESO will grade each answer sheet and notify you of any incorrect answers. The passing score for each assignment is 3.2. If you receive less than 3.2 on any assignment, your ESO will list the questions you answered incorrectly and give you an answer sheet marked

"RESUBMIT." You must redo the assignment and complete the RESUBMIT answer sheet. The maximum score you can receive for a resubmitted assignment is 3.2.

COURSE COMPLETION: After you have submitted all the answer sheets and have earned at least 3.2 on each assignment, your command should give you credit for this course by making the appropriate entry in your service record.

NAVAL RESERVE RETIREMENT CREDIT: If you are a member of the Naval Reserve, you will receive retirement points if you are authorized to receive thereunder current directives governing retirement of Naval Reserve personnel. For Naval Reserve retirement, this course is evaluated at 8 points. (Refer to BUPERSINST 1001.39 for more information about retirement points.)

STUDENT QUESTIONS: If you have questions concerning the administration of this course, consult your ESO. If you have questions on course content, you may contact NETPDTC at:

DSN: 922-1501
Commercial: (904) 452-1501
FAX: 922-1819
INTERNET:
n311.products@smtp.cnet.navy.mil

COURSE OBJECTIVES: In completing this nonresident training course, you will demonstrate a knowledge of the subject matter by correctly answering questions on the following subjects:

AIS Administration, Communications Administration, Communications Security, AIS Security, and General Security.

Naval courses may include several types of questions--multiple-choice, true-false, matching, etc. The questions are not grouped by type but by subject matter. They are presented in the same general sequence as the textbook material upon which they are based. This presentation is designed to preserve continuity of thought, permitting step-by-step development of ideas. Not all courses use all of the types of questions available. You can readily identify the type of each question, and the action required, by reviewing of the samples given below.

## MULTIPLE-CHOICE QUESTIONS

Each question contains several alternative answers, one of which is the best answer to the question. Select the best alternative, and blacken the appropriate box on the answer sheet.

SAMPLE

s-1. The first U.S. Navy nuclear-powered vessel was what type of ship?

1. Carrier
2. Submarine
3. Destroyer
4. Cruiser

Indicate in this way on your answer sheet:

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| | T | F | | |
| s-1 | ☐ | ■ | ☐ | ☐ |

## TRUE-FALSE QUESTIONS

Mark each statement true or false as indicated below. If any part of the statement is false, the entire statement is false. Make your decision, and blacken the appropriate box on the answer sheet.

SAMPLE

s-2. Shock will never be serious enough to cause death.

1. True
2. False

Indicate in this way on your answer sheet:

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| | T | F | | |
| s-2 | ☐ | ■ | ☐ | ☐ |

## MATCHING QUESTIONS

Each set of questions consists of two columns, each listing words, phrases or sentences. Your task is to select the item in column B which is the best match for the item in column A. Items in column B may be used once, more than once, or not at all. Specific instructions are given with each set of questions. Select the numbers identifying the answers and blacken the appropriate boxes on your answer sheet.

SAMPLE

In answering questions s-3 through s-6, SELECT from column B the department where the shipboard officer in column A functions. Responses may be used once, more than once, or not at all.

| A. OFFICER | B. DEPARTMENT |
|---|---|
| s-3. Damage Control Assistant | 1. Operations Department |
| s-4. CIC Officer | 2. Engineering Department |
| s-5. Disbursing Officer | 3. Supply Department |
| s-6. Communications Officer | 4. Navigation Department |

Indicate in this way on your answer sheet:

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| | T | F | | |
| s-3 | ☐ | ■ | ☐ | ☐ |
| s-4 | ■ | ☐ | ☐ | ☐ |
| s-5 | ☐ | ☐ | ■ | ☐ |
| s-6 | ■ | ☐ | ☐ | ☐ |

# ASSIGNMENT 1

Textbook Assignment: "AIS Administration," chapter 1, pages 1-1 through 1-28.

---

1-1. You are working as an I/O control clerk. Before accepting a job for processing on the computer, you should look over the transmittal form to ensure which of the following criteria is met?

1. All copies have been filed
2. All entries are readable and understandable
3. All required outputs have been specified
4. All SCL statements are in the proper sequence

1-2. Computer operations has just informed you that the payroll update (a series of 18 jobs) is finished and ready for pickup. Upon receiving the output, you should take what action immediately?

1. Use the burster
2. Log the jobs out
3. File the jobs
4. Check the output products

1-3. As an I/O control clerk, you will NOT be expected to perform which of the following tasks?

1. Make SCL changes to production run streams
2. Monitor jobs to ensure all data-are processed
3. Reconcile processing discrepancies and inconsistencies
4. Assist the computer operator in setting up production jobs

1-4. As an I/O control clerk, you can be expected to operate a variety of equipment, such as copying machines, and terminals. These are known as what type of equipment?

1. Online
2. Auxiliary
3. Secondary
4. Independent

1-5. On the transmittal form, the block marked "OPERATIONS USE ONLY" contains which of the following items of information?

1. Job/task number
2. Computer to be used
3. Type of operation performed
4. When the job was accepted

1-6. As an I/O control clerk, one of your jobs will be to keep an up-to-date record of all jobs received for processing. What document should you use?

1. A run schedule
2. A job schedule
3. A pass down log
4. A job control log

1-7. If the input that comes with a job becomes misplaced or lost, you still have means of tracking it down by lookinq in what control log entry?

1. Program name
2. Type of input
3. Input forwarded
4. Computer system

1-8. To properly prepare the user's input for processing, you as I/O control clerk must have a certain amount of information available, such as computer run sheet, how to make up control or SCL statements, and any special output requirements the job may call for. This information can be found in the

1. run book
2. job manual
3. task folder
4. master run manual

1-9. A run sheet to be used by the computer operator should contain which of the following information?

1. Breakpoints
2. Partition numbers
3. Recovery procedures
4. List of required inputs

1-10. If a job terminates before going to a normal EOJ, you as the I/O control clerk may be required to collect which of the following data/information?

1. Output data and memory dump only
2. Input data and SCL statements only
3. Input data, output data, and memory dump
4. Output data, console printout, and SCL statements

1-11. During the SUADPS daily update for supply, problems reading the current master read file (MRF) on disk drive 241 are encountered. The job terminates prematurely, leaving eight jobs to be run. The computer operator calls on you as the I/O control clerk to help in the recovery process. You can be expected to perform all except which of the following tasks?

1. Provide the operator with the input parameters and/or SCL statements to recover the job
2. Remove the defective disk pack from drive 241 and forward it to the technicians to be checked out
3. See to it that the remaining jobs are rescheduled once the master file is recreated, and notify the user
4. Provide the operator with the file identification number needed to recover the MRF file

1-12. As an I/O control clerk, to determine that a job ran successfully and that all processing steps were properly carried out, you should review what document?

1. The pass down log
2. The computer run sheet
3. The confirmation report
4. The computer console printout

1-13. As an I/O control clerk, what document provides you with a list of all the error conditions and messages for all jobs run on the computer during a work shift?

1. The error/discrepancy report
2. The computer console printout
3. The error message log
3. The rerun report

1-14. As an I/O control clerk, you may be responsible for reconciling processing discrepancies . To determine the problem, which of the following documents will usually provide you with the information you need?

1. The pass down log
2. The computer run sheet
3. The confirmation report
4. The computer console printout

1-15. As an I/O control clerk, you are checking over the user's output products and need to verify that all items requested were produced. To do this, you should refer to which of the following sources?

1. The run manual
2. The task folder
3. The user manual
4. The instruction folder

1-16. As an I/O control clerk, once you have packaged the user's output products and placed them in the pick-up area, you should log the job out in which of the following logs?

1. The job control log
2. The user's job log
3. The production log
4. The EOJ/pick-up log

1-17. As an I/O control clerk, if during the process of checking over the user's output products, you happen to come across an error, you should carry out which of the following actions?

1. Log the job out, and inform the user of the error at the time of pickup only
2. Bring the error to the attention of your superior, then log the job out with the appropriate comments only
3. Reschedule the job as if nothing has happened, and notify the user there will be a slight delay
4. Pull the job immediately, bring the error to the attention of your superior so the job may be rescheduled, and notify the user

1-18. As an I/O control clerk, You will be involved with and communicating with the user. Which of the following communications skills must you possess in order to maintain a good relationship with the user?

1. Refer problems to users
2. Explain problems only
3. Understand requests only
4. Understand requests and explain problems

1-19. A scheduler does NOT perform which of the following tasks?

1. Review AIS requests
2. Prepare schedules
3. Operate the computer to run production jobs
4. Organize data processing priorities for both scheduled and unscheduled work

1-20. What method should you use to determine the accuracy of your schedules?

1. Monitor the jobs
2. Review production results
3. Supervise computer operations
4. Review job control logs

1-21. To determine how to go about scheduling work on your facility's computer system, you should depend on which of the following factors?

1. The number of jobs to be scheduled
2. The system configuration only
3. The operating mode of the system only
4. The system configuration and operating mode

1-22. Which of the following is NOT an example of a computer operating mode?

1. Prime-time
2. Real-time
3. Online
4. Batch

1-23. As scheduler, you will be concerned with precomputer processing for which of the following reasons?

1. To see that the work is performed accurately
2. To see that sufficient magnetic media are available to store the data
3. To ensure that all inputs are received on time according to prearranged schedules
4. To ensure users are complying with standard operating procedures

1-24. If you schedule so much work for the computer that you overload the computer system, which of the following results is likely to occur?

1. AIS services are underutilized
2. User service deteriorates
3. Precomputer processing service deteriorates
4. Each of the above

1-25. As a scheduler, which of the following factors must you know about the files in use?

1. Where to find them in the magnetic media library
2. Where to store them in the magnetic media library
3. The record sizes and blocking factors of each file
4. How to reconstruct them

1-26. As a scheduler, what information must you know about the jobs you are to schedule?

1. How jobs interface only
2. How much time it takes to run each job only
3. How jobs interface and how much time it takes to run each job
4. How to operate the computer to back up production jobs

1-27. As a scheduler, you do NOT have to be proficient in which of the following skills?

1. Sound judgment
2. Tact and diplomacy
3. Analytical ability
4. Systems design

1-28. Production control acts as liaison between the AIS facility and the user community to perform which of the following functions?

1. Provide magnetic media support to the user
2. Provide programming services to the user
3. Adjust data flow and output schedules based on user and production requirements
4. Determine if errors are caused by hardware or systems/applications software

1-29. What functional area receives incoming work and checks to be sure the amount of input data is approximately the amount indicated on the production schedule?

1. Technical support
2. Quality control
3. I/O control
4. Data entry

1-30. Source documents are received and processed by what (a) functional area, and checked for completeness and accuracy by what (b) functional area?

1. (a) Data entry
   (b) Quality control
2. (a) Data entry
   (b) Technical support
3. (a) Scheduling
   (b) Quality control
4. (a) Scheduling
   (b) Technical support

1-31. To chart the interaction between the functional areas of an AIS facility, what type of chart should you prepare?

1. Data flowchart
2. Systems flowchart
3. Workload diagram
4. Workflow diagram

1-32. To determine what the demands will be on the AIS facility for the upcoming month, which of the following personnel usually meet(s) with the users?

1. Division chief only
2. Division chief and LPO only
3. Division chief, LPO, and scheduler
4. Computer operations supervisor and scheduler

1-33. During the forecasting phase of scheduling, you must remember to set aside time in the schedule for which of the following maintenance tasks?

1. File and computer
2. Tape drive
3. Disk drive
4. Each of the above

1-34. When you schedule recurring (old) jobs, which of the following types of information is/are best to use?

1. New estimates from users
2. Job experience and history
3. Latest job run time on your system
4. Average job run time on other systems

1-35. Scheduling enables management to make which of the following judgments?

1. A prediction of the effects of an increased workload
2. An evaluation of data entry operator skills
3. An analysis of production program errors
4. A plan for user training

1-36. As scheduler, you will need a backup or contingency plan for which of the following reasons?

1. To allow for hardware breakdowns and malfunctions
2. To schedule users' requirements
3. To allow for late submission of input from the user
4. To correct job parameters that are entered into the system incorrectly

1-37. Resource requirements, processing time, job dependencies, priorities, and deadlines are all what type of information?

1. Job-related
2. Workload-related
3. Resource-related
4. AIS facility-related

1-38. As scheduler, in addition to having information about computer resources, you need information about what other area(s) of processing?

1. Precomputer processing only
2. Postcomputer processing only
3. Precomputer and postcomputer processing
4. Output processing by users

1-39. What is the primary difficulty of manually scheduling jobs in a multiprogramming environment?

1. Specifying priorities
2. Specifying deadlines
3. Obtaining a job mix that handles job dependencies without processing jobs out of order
4. Obtaining a job mix that makes the best use of most resources without bogging down the entire computer system

2-40. Resources, workflow, system capabilities and capacities, and workload demands are all what type of information?

1. Job-related
2. Workload-related
3. Resource-related
4. AIS facility-related

1-41. To be sure sufficient time is scheduled for a job, you will probably want to add extra time to the estimated time as a safety factor. What is this type of time called?

1. Excess time
2. Time-plus
3. Real time
4. Buffer time

1-42. As scheduler, to provide for priority changes, special job requests, power outages, and corrective maintenance, you must take which of the following actions?

1. Reboot the computer system quickly without operator assistance
2. Readjust schedules quickly with a minimum of disruption
3. Revise your normal scheduling procedures to avoid these problems
4. Request scheduling assistance from computer operations personnel

1-43. When preparing a monthly schedule, you should be sure to include time for which of the following requirements?

1. Testing only
2. Planned maintenance only
3. Backup procedures only
4. Testing, planned maintenance, and backup procedures

1-44. Which of the following things do NOT normally affect the approved monthly schedule?

1. System backups
2. Software testing
3. System/program errors
4. Input files not available

1-45. A work load schedule is which of the following types of schedules?

1. External only
2. Internal only
3. External and internal

1-46. During production processing, monitoring the jobs to see that the work is being accomplished as planned is the responsibility of all except which of the following personnel?

1. Operator
2. I/O control clerk
3. Technical administrator
4. Production control coordinator

1-47. Who is the most qualified and highly trained individual to assist online users with their particular processing problems?

1. Operator
2. Shift supervisor
3. Production control clerk
4. Subsystem coordinator

1-48. Which of the following problems is one of the most frequent hardware problems associated with production processing?

1. Loss of power
2. Printer out of paper
3. Tape read/write errors
4. Wrong printer forms loaded

1-49. Which of the following problems is NOT a common external environmental problem?

1. Head crash
2. Loss of power
3. Voltage spikes
4. Loss of air conditioning

1-50. To correct software related problems, the operator must refer to which of the following sources for the corrective action to take?

1. Program operator manual only
2. Job run folder only
3. Program operator manual and job run folder
4. System manual

1-51. Unscheduled downtime can result from all except which of the following causes?

1. Power failures
2. Rebooting the system
3. Loss of air conditioning
4. System saves

1-52. When a software problem is researched, which of the following items is the most important?

1. Abort code
2. Program step
3. Action taken
4. Date job submitted

1-53. To improve performance and operation, you should provide feedback to all but which of the following people?

1. Shift supervisor
2. I/O control clerk
3. Technical administrator
4. Production control coordinator

1-54. To improve system performance, you can look for trends in the production process. Which of the following trends would NOT be looked at?

1. Impact of modified applications
2. Times when system was idle
3. Backlog of jobs to be run
4. Times when system seems slow

1-55. The amount of information you include in an AIS report should NOT exceed whose requirements?

1. User’s
2. Supervisor’s
3. Facility manager’s
4. Upper management’s

1-55. Which of the following items is NOT required in an ASDP?

1. Outline of the need
2. Prediction of the future need
3. Summary of the selected FIP resource solution
4. Summary of the projected costs

1-57. Downtime reported on the hardware utilization report includes which of the following types of downtime?

1. Whole system only
2. Each piece of equipment only
3. Whole system and each piece of equipment as appropriate
4. Equipment awaiting installation

1-58. Hardware under-utilization can be measured by excessive idle time.

1. True
2. False

1-59. Which of the following situations is NOT usually a cause of application software aborts?

1. File corrupted
2. File not available
3. Job run in sequence
4. Out of free disk space

1-60. Which of the following reports are good sources for determining what performance-tuning techniques to implement?

1. Hardware and software projection
2. Application software performance
3. Hardware utilization
4. Operating system software

1-61. With average program mixes, cache memory can-yield what percent increase in processing speed?

1. 30%
2. 40%
3. 50%
4. 60%

1-62. You can make all but which of the following changes to the operating system?

1. Change memory addresses
2. Reconfigure disk drives
3. Reconfigure the system
4. Change buffer sizes

1-63. When submitting a trouble report, you must follow the instruction from which of the following commands?

1. The type commander
2. The command receiving the trouble report
3. The command sending the trouble report

1-64. When you cannot work around a problem to continue operating, what priority should you assign to the trouble report?

1. Critical
2. Routine
3. Urgent

1-65. When you can work around the problem but a resolution is required immediately, what priority should you assign to the trouble report?

1. Critical
2. Routine
3. Urgent

1-66. All of the following are common reasons for the submission of a hardware trouble report except which one?

1. System keeps locking up
2. System keeps dropping I/O channels
3. Corrupted file and no save tapes are available
4. Bad data entered in file

l-67. When preparing the operational guidelines for your facility, which of the following areas should you consider?

1. Backup operations only
2. Contingency plans and disaster recoveries only
3. Emergency responses only
4. Backup operations, contingency plans and disaster recoveries, and emergency responses

1-68. Which of the following is NOT a common reason for urgent change requests?

1. Changes to the operating system
2. Equipment degradation
3. System testing
4. Special saves

# ASSIGNMENT 2

Textbook Assignment: "Communications Administration," chapter 2, pages 2-1 through 2-29.

---

2-1. DCS circuits are owned or leased by what organization?

1. AT&T
2. The Joint Military Communications Management Office
3. The U.S. Government
4. NAVCOMTELCOM

2-2. The DCS combines elements from the three military services into a single communications system.

1. True
2. False

2-3. Who exercises operational control over the DCS?

1. The civilian head of the DCA
2. The head of the JCS
3. The military head of the NTS
4. The military head of DISA

2-4. What is the mission of naval communications?

1. To provide reliable, secure, and rapid communications
2. To provide reliable, simple, and rapid communications
3. To provide controlled, secure, and functional communications
4. To provide easy, secure, and rapid communications

2-5. Naval communications includes which of the following policies?

1. To promote the safety of life at sea and in the air by maintaining communications with appropriate communications facilities
2. To encourage at all levels of command an effort to improve techniques, procedures, and efficiency
3. To establish and maintain effective communications within the Department of the Navy
4. Each of the above

2-6. Concerning area of coverage, what is the primary distinction between the NTS and the DCS?

1. The DCS units are fleet associated, and the NTS facilities are primarily ashore
2. The NTS facilities are fleet associated, and the DCS units are primarily ashore
3. Navy teleprinter communications are within the realm of the NTS; Navy communications by any other means are under the cognizance of the DCS
4. Navy teleprinter communications are within the realm of the DCS; Navy communications by any other means are under the cognizance of the NTS

2-7. Who is responsible for operational and management control of the elements of the NTS?

1. Commander, Naval Support Force
2. Commander, Naval Computer and Telecommunications Command
3. Commander in Chief, Atlantic Fleet
4. Chief of Naval Operations

2-8. How do fleet commanders assign communications responsibilities to their respective fleets?

1. Communications Information Bulletins (CIBs)
2. Wide Area Network (WAN)
3. Operation Orders (OPORDs)
4. Naval messages

2-9. The world is divided into what total number of Nava] Communications Areas (NAVCOMMAREAS)?

1. Five
2. Six
3. Three
4. Four

2-10. Who exercises coordination and control of all naval communications within each NAVCOMMAREA?

1. Officer in Charge, NAVCOMMAREA
2. Naval Computer and Telecommunications Area Master Station
3. The fleet CINC in the area
4. Naval Communications Station

A. NCTAMS
B. NAVCOMTELSTA
C. NAVCOMTELDET
D. NAVSECGRUDEPT

Figure 2A

IN ANSWERING QUESTIONS 2-11 THROUGH 2-14, SELECT FROM FIGURE 2A THE NAVAL TELECOMMUNICATIONS COMMAND ELEMENT DESCRIBED.

2-11. Assigned a limited or specialized mission.

1. A
2. B
3. C
4. D

2-12. Responsible for cryptologic operations.

1. A
2. B
3. C
4. D

2-13. Entry point for Navy Tactical Satellite Systems.

1. A
2. B
3. C
4. D

2-14. Provides Naval Industrial Fund ADP services.

1. A
2. B
3. C
4. D

2-15. When you are assigned as a communications manager, what should be your first consideration?

1. Compare the communications organization with others of similar size
2. Evaluate the effectiveness of organization' s communications
3. Evaluate the personnel training program
4. Rotate personnel in their jobs to improve training

2-16. To measure the effectiveness of the operations and services-provided by your communications facility, you should establish standards of performance for which of the following areas?

1. Speed
2. Security
3. Reliability
4. A1l of the above

2-17. Fixed standards for work measurement processes present what potential problem?

1. They may prevent changes that are needed as a result of changing conditions
2. They limit variety in work assignments
3. They tend to limit individual work potential
4. They allow for individual initiative, which is undesirable

2-18. To overcome resistance to changes in performance standards, which of the following methods is recommended?

1. Show the personnel concerned how wasteful their former methods were
2. Give personnel a complete description of the changes being made
3. Permit personnel who will be-affected by the changes to participate in the organizing effort
4. Advise the personnel concerned that they must overcome their natural resistance to change

2-19. You may improve overall personnel performance by evaluating which of the following factors?

1. Personnel requirements
2. Existing organizational structure
3. Both 1 and 2 above
4. The need for qualified replacements

2-20. A lack of efficiency in a communications division is a direct reflection of the management skills of which of the following individuals?

1. Commanding officer
2. Senior supervisor
3. Training officer
4. Watchstanders

2-21. To reorganize divisional workflow and workspace layout, what information do you need to plan properly?

1. What work is to be done
2. When the work is to be performed
3. HOW the work is to be accomplished
4. Each of the above

2-22. What is a major responsibility of a supervisor?

1. Promote timeliness
2. Monitor production
3. Maintain proper work hours
4. Ensure personnel are fit

2-23. When office layout is being planned, what is the primary consideration?

1. Security of classified material
2. Safety factors
3. Number of personnel to be accommodated
4. Proper flow of paper and work

2-24. The physical layout of your office should be arranged so that paperwork will flow in what direction(s)?

1. One direction
2. A clockwise direction
3. Back-and-forth
4. Two directions at once

2-25. What publication lists the types of ships that are required to have a communications department?

1. NWP 1 (NWP 2-01)
2. ACP 100
3. NWP 4 (NWP 6-01)
4. NTP 4

2-26. Who is responsible to the communications officer for compliance with communications directives and for the accurate and rapid handling of messages?

1. Communications watch officer
2. Senior watch supervisor
3. Communications center supervisor
4. Technical control supervisor

2-27. Who directly supervises all radiomen on watch in the message processing area and is responsible for notifying the CWO and SWS on any unusual or urgent matters?

1. Assistant watch supervisor
2. Radio officer
3. Communications center supervisor
4. Technical control supervisor

2-28. Who is responsible for examining operational logs, monitoring equipment alignment and operation, and preventing message backlogs?

1. Communications center supervisor
2. Senior watch supervisor
3. Radio officer
4. Technical control supervisor

2-29. Who has full responsibility for the internal handling of message traffic within the ship?

1. Commanding officer
2. Executive’ officer
3. Communications officer
4. Radio officer

2-30. Who is responsible for the organization, supervision, and coordination of the command's external communications?

1. Radio officer
2. Communications officer
3. Communications watch officer
4. Communications watch. supervisor

2-31. Who is responsible for preparing and maintaining the communications watch, quarter, and station bill?

1. Communications officer
2. Communications watch officer
3. Radio officer
4. Senior watch supervisor

2-32. Who is responsible for maintaining the status board which displays equipment, nets, and circuit information?

1. Communications officer
2. Communications center supervisor
3. Senior watch supervisor
4. Technical control supervisor

2-33. Who is responsible for managing the command's CMS account and for advising the commanding officer on all matters concerning CMS?

1. Communications officer
2. Radio officer
3. Crypto officer
4. CMS officer

2-34. Directives issued by naval commanders to effect the coordinated execution of an operation are known by what term?

1. Communications plan (COMMPLAN)
2. Execution order (EXORD)
3. operation order (OPORD)
4. Standard operating procedure (SOP)

2-35. An OPORD is made up of what three parts?

1. Heading, plan, and closure
2. Beqinning, body, and annex
3. Heading, body, and closure
4. Heading, body, and ending

2-36. Detailed information for various ship departments is contained in what two enclosures?

1. Annexes and appendices
2. Annexes and tabs
3. Appendices and indexes
4. Annexes and indexes

2-37. A document issued by an organization to advise its personnel of internal routine practices is most commonly issued in what format?

1. Division instruction
2. Division officer instruction
3. Standard operating procedure
4. Operational instruction

2-38. How detailed a standard operating procedure (SOP) is depends on which of the following factors?

1. The state of training
2. The complexity of the instructions
3. The size of the command
4. Each of the above

4-39. What type of message is destined for two or more addressees, none of whom is informed of any other addressee?

1. Book
2. General
3. Multiple-address
4. Single-address

4-40. What type of message has a wide, predetermined, standard distribution?

1. Book
2. General
3. Multiple-address
4. Single-address

2-41. How can four-letter address groups be distinguished from Navy four-letter international radio call signs?

1. Address groups are transmitted with a hyphen between the first and second letters
2. Address groups are transmitted with a hyphen between the third and fourth letters
3. Address groups are always transmitted twice
4. Address groups do not begin with the letter N

4-42. What type of address group must always have more information added to it to serve as a complete station and address designator?

1. Individual activity address group
2. Collective address group
3. Conjunctive address group
4. Address indicating group

4-43. What always precedes geographic address groups?

1. Individual activity address groups
2. Collective address groups
3. Conjunctive address groups
4. Address indicating groups

4-44. What is the purpose of address indicating groups (AIGs)?

1. To reduce the number of address groups required in the heading of a message
2. To convey special instructions in the heading of a message
3. To provide an alternate address group in the event that the primary address group is compromised
4. To locate the originator of a message geographically

4-45. A single address group that represents a set of four or more activities, including the cognizant authority, is known by what term?

1. Conjunctive address group
2. Collective address group
3. Collective address desiqnator
4. Call-sign

2-46. The Navy uses GMT as a common 24-hour worldwide time standard in messages for the date-time group and time of file. What does GMT stand for?

1. Greenwich Mean Time
2. General Master Time
3. Greenwich Master Time
4. Global Mean Time

2-47. The world is divided into what total number of GMT time zones?

1. 6
2. 12
3. 24
4. 48

2-48. The time zone which passes through Greenwich, England, is most commonly known by what term?

1. GREEN time zone
2. ROMEO time zone
3. YANKEE time zone
4. ZULU time zone

2-49. If you were stationed in time zone ROMEO, how would you convert (a) local time to GMT and (b) GMT to local time?

1. (a) Subtract 5 hours from local time
   (b) add 5 hours to GMT
2. (a) Add 5 hours to local time
   (b) subtract 5 hours from GMT
3. (a) Subtract 5 hours from GMT
   (b) add 5 hours to local time
4. (a) Add 5 hours to GMT.
   (b) subtract 5 hours from local time

2-50. An eastbound ship crossing the international date line loses a day.

1. True
2. False

2-51. What is an important point to remember about the MIKE and YANKEE zones?

1. The day changes along with the time, plus or minus 1 hour
2. The day remains the same, but the time changes, plus or minus 1 hour
3. The day and the time remain the same
4. The day changes, but the time remains the same

2-52. How many digits make up the Julian date?

1. Nine
2. Seven
3. Six
4. Four

2-53. The precedence of a message should be based on what factor?

1. The urgency of the message
2. The classification of the message
3. The number of addressees who are to receive the message
4. The importance of the subject matter

2-54. What is the highest precedence that is normally authorized for administrative messages?

1. Routine
2. Priority
3. Immediate
4. Flash

2-55. What precedence is assigned to a message that is of such urgency that it must be brief?

1. Priority
2. Immediate
3. Yankee
4. Flash

2-56. What precedence is limited to designated emergency action command and control messages within the AUTODIN system?

1. Priority
2. Immediate
3. Flash
4. Yankee

2-57. Composing a message and selecting the proper classification and precedence is the responsibility of what individual?

1. The drafter
2. The releaser
3. The originator
4. The commanding officer

2-58. Before accepting a message originated in or destined for an area under minimize for transmission, the outrouter must ensure that which of the following information is on the message?

1. The notation “MINIMIZE CONSIDERED” in the appropriate area of the message form
2. The releaser’s name and rank/grade in the last line of the message text
3. Both 1 and 2 above
4. The notation “MINIMIZE CONSIDERED” stamped on the message form or diskette

2-59. Which of the following messages are used to determine delay or nondelivery of a message on a station-to-station basis?

1. Pro forma
2. Service only
3. Tracer only
4. Both service and tracer

2-60. Which of the following messages are described as short and concise messages between operators dealing with message corrections, broadcast reruns, and missent or misrouted messages?

1. Pro forma
2. MINIMIZE
3. Service only
4. Service and tracer

2-61. Where does an activity send the results of a tracer investigation?

1. To the originator of the tracer message only
2. To the preceding station(s) only
3. To the originator of the tracer message and the preceding station(s) only
4. To the originator of the tracer message, the preceding station(s), and the following station

2-62. To establish a termination with a NCTAMS or NAVCOMTELSTA, a ship must send a request what minimum time in advance?

1. 24 hr
2. 48 hr
3. 72 hr
4. 96 hr

2-63. When it needs to shift broadcast guard, a ship sends what type of message?

1. Termination request message
2. Communications guard shift
3. Service message
4. Broadcast screen request

2-64. Broadcast screen requests should be sent to what organization?

1. Broadcast rerun station
2. Broadcast radiating station
3. Broadcast control station
4. Broadcast keying station

2-65. A COMMSPOT report should be sent under what circumstances?

1. As soon as unusual communication difficulties arise
2. As soon as communication difficulties are corrected
3. Whenever unusual communication difficulties are expected
4. Durinq solar flare-ups

2-66. What type of message is placed in the cryptocenter file?

1. SPECAT
2. SPECAT SIOP-ESI
3. TICON
4. NATO

A. Authentication

B. Codes

C. Ciphers

D. Radio silence

E. Monitoring

F. Identification Friend or Foe (IFF)

Figure 2A

IN ANSWERING QUESTIONS 2-67 THROUGH 2-72,SELECT THE SECURITY DEVICE OR PROCEDURE FROM FIGURE 2A THAT IS BEST DESCRIBED IN THE QUESTION.

2-67. Any cryptologic system in which arbitrary symbols or groups of symbols represent units of plain text.

1. A
2. C
3. E
4. F

2-68. Uses electromagnetic transmissions to which equipment carried by friendly forces automatically respond.

1. B
2. C
3. E
4. F

2-69. A procedure designed to protect communications systems against acceptance of false transmissions or simulations by establishing the validity of a transmission, message, or originator.

1. A
2. B
3. C
4. D

2-70. A system of communication in which arbitrary groups of symbols represent units of plain text; used for brevity and/or security.

1. A
2. B
3. C
4. E

2-71. A condition in which all or certain radio equipment is kept inoperative.

1. A
2. B
3. C
4. D

2-72. The act of listening, carrying out surveillance on, and/or recording the emissions of own or allied forces.

1. A
2. B
3. E
4. F

2-73. The communications plan satisfies communications requirements by providing what information?

1. Specifies circuit operators, equipment, and traffic capabilities
2. Establishes watchbills, software requirements, and deployment times
3. Designates enemy communications frequencies, supporting COMMSTAs, and supply requirements
4. Specifies circuits, channels, and facilities to be used

2-74. What document initiates the addition, deletion, or change to an existing DCS circuit?

1. Telecommunications Service Order (TSO)
2. Telecommunications Service Request (TSR)
3. Circuit Service Transfer (CST)
4. Request for Modification of Circuit (RMC)

# ASSIGNMENT 3

Textbook Assignment: "Communications Administration (continued)," chapter 2, pages 2-29 through 2-37; "Communications, Security," chapter 3, pages 3-1 through 3-12; "AIS Security," chapter 4, pages 4-1 through 4-12.

---

3-1. If you desire to delete an existing DCS circuit, you should submit what type of request?

1. An AUTODIN deletion request
2. A telecommunications service request
3. A DCA circular request
4. A technical control service request

3-2. Requirements for new telecommunications services should be defined and submitted what minimum time in advance?

1. 1 yr
2. 2 yr
3. 3 yr
4. 6 mo

3-3. What does a TSO authorize?

1. Funding to begin basic circuit design
2. Starting, changing, or discontinuing circuits
3. Procurement of specific devices or ancillary equipment
4. Both 2 and 3 above

3-4. Navy funds cannot be obligated for developing or procuring communications equipment that uses a portion of the frequency spectrum until what is obtained?

1. Frequency usage estimate
2. A frequency allocation
3. A spectrum study
4. An FCC recommendation

3-5. Which of the following constraints should be considered when a frequency assignment is authorized?

1. Power, emission bandwidth, location of antennas, and operating time
2. Power, receiver locations, and atmospheric conditions
3. Bandwidth, sidebands, harmonics, and power requirements
4. Power, harmonics, and RF hazards to personnel

3-6. What authority grants Navy and Marine Corps activities within the U.S. permission to use radio frequencies?

1. Naval Electromagnetic Spectrum Center (NAVEMSCEN)
2. National Telecommunications and Information Administration (NTIA)
3. United States Military Communications Electronics Board (USMCEB)
4. Chief of Naval Operations (CNO)

3-7. In the Navy, what organization authorizes frequency assignment applications?

1. The United States Military Communications Electronics Board (USMCEB)
2. The National Telecommunications and Information Administration (NTIA)
3. The Joint Chiefs of Staff
4. The Naval Electromagnetic Spectrum Center (NAVEMSCEN)

3-8. Who is authorized to send PERSONAL FOR messages?

1. E-7 military or GS-7 civilian (or above)
2. Officers of flag rank or in a command status only
3. All officers
4. Anyone who needs to send a personal message

3-9. What is contained in the publications in the NWPL?

1. Manning plans, battle organizations, and future deployment schedules
2. Awards information, maintenance schedules, and supply information
3. Required procedures, signals, and other operational and mission-essential information
4. Operational requirements, battle organizations, and deployment schedules

3-10. What is the objective of the central administration of the NWPL?

1. To ensure that the publications in the NWPL are correct and readily avail-able for use
2. To ensure that personnel have a place to study for advancement
3. To ensure that personnel have access to publications and periodicals on the latest technology
4. To ensure that personnel have access to the most recent and best-selling novels

3-11. Who is responsible for the management of the NWPL?

1. The naval warfare publications officer
2. The naval warfare publications custodian
3. The naval warfare publications librarian
4. The naval warfare publications manager

3-12. What publication provides guidance for the administration and security of the NWPL?

1. OPNAVINST 5510.1
2. NTP 4
3. NWP 4 (NWP 6-01)
4. NWP 0 (NWP 1-01)

3-13 . Who is responsible for changes or corrections to NWPL publications?

1. The NWPL clerk
2. The primary user
3. The NWPL custodian
4. The communications watch officer

3-14. Who is considered to be a holder under the administration of NWPL?

1. A person who holds NWPL publications for short terms only
2. A person who transports publications to and from the NWPL
3. A person who has permanent subcustody of publications from the NWPL
4. The NWPL custodian

3-15. Which of the following files are used in NWPL maintenance?

1. Signature and custody fries
2. Administrative and transaction files
3. Signature and administrative files
4. Custody and administrative files

3-16. The NWPL administrative file is also known by what other term?

1. Transaction file
2. Office file
3. A-1 file
4. Custody file

3-17. Material in the administrative file must be retained for what minimum time ?

1. 1 yr
2. 2 yr
3. 5 yr
4. 6 mo

3-18. What colors are assigned to the binders for U.S. naval warfare publications of different classifications?

1. Secret - red, Confidential - green, Unclassified - white
2. Secret - red, Confidential - yellow, Unclassified - blue
3. Secret - red, Confidential - yellow, Unclassified - white
4. Secret - red, Confidential - green, Unclassified - blue

3-19. Where is the effective date of the publication change/correction found?

1. In the Record of Changes page
2. In the List of Effective Pages (LOEP)
3. In the Foreword or Letter of Promulgation
4. In the Title page

3-20. Which of the following colors should be used to make pen-and-ink corrections to NWPL publications?

1. Green only
2. Black or blue only
3. Any dark color except red
4. Any color is acceptable

3-21. What does the designation "NMC 6/2" on a correction mean?

1. It is the 6th message correction and will-be incorporated into the publication by printed change number 2
2. It is the 2nd message correction and will be incorporated into the publication by printed change number 6
3. It was sent on the 2nd of June of the current year
4. It is the 6th change to the 2nd revision of the publication

3-22. What document contains guidance for taking extracts from a NATO publication?

1. OPNAVINST 5510.1
2. ACP 121
3. NWP 0 (NWP 1-01)
4. NATO letter of promulgation

A. ACPs
B. NTPs
C. JANAPs
D. NWPs

Figure 3A

IN ANSWERING QUESTIONS 3-23 THROUGH 3-26, SELECT THE PUBLICATIONS FROM FIGURE 3A THAT ARE DESCRIBED.

3-23. Provide communications instructions and procedures essential to conducting combined military operations in which two or more allied nations are involved.

1. A
2. B
3. C
4. D

3-24. Coordinate and standardize communications procedures among U.S. military services.

1. A
2. B
3. C
4. D

3-25. Main publications used by Navy, Coast Guard, and Marine personnel for communications.

1. A
2. B
3. C
4. D

3-26. Incorporate the results of fleet tactical development and evaluation programs and NATO experience and provide information about the tactical capabilities and limitations of equipment and systems.

1. A
2. B
3. C
4. D

A. CMS account
B. CMS custodian
C. CMS local holder
D. CMS user

Figure 3B

IN ANSWERING QUESTIONS 3-27 THROUGH 3-29, SELECT THE TERM FROM FIGURE 3B THAT IS DESCRIBED.

3-27. A command with an account number that draws its COMSEC material directly from national or Navy distribution sources.

1. A
2. B
3. C
4. D

3-28. COMSEC material needs are met by drawing such material from the squadron commander.

1. A
2. B
3. C
4. D

3-29. An individual who requires the use of COMSEC material for a short time to accomplish a specific task.

1. A
2. B
3. C
4. D

3-30. Which of the following statements concerning storage requirements for COMSEC material is/are correct?

1. COMSEC material may be stored with other communications material according to security classification
2. COMSEC material must be stored separately from non-COMSEC material
3. COMSEC material of different classification may be stored. together regardless of classification if storage limitations are a factor
4. Both 2 and 3 above

3-31. What number of signatures is/are required on the COMSEC watch-to-watch inventory sheet?

1. One
2. Two
3. Three
4. Four

3-32. What is the maximum length of time that you are authorized to hold superseded (a) keying material marked CRYPTO and (b) authentication publications?

1. (a) 24 hours (b) 24 hours
2. (a) 12 hours (b) 5 days
3. (a) 5 days (b) 12 hours
4. (a) 5 days (b) 5 days

3-33. What are the three types of keying material in descending priority of destruction?

1. Superseded, reserve, effective
2. Effective, superseded, reserve
3. Reserve, effective, superseded
4. Superseded, effective, reserve

3-34. Effective keying material is the most sensitive of the three types of keying material.

1. True
2. False

3-35. What is the purpose of Two-Person Integrity?

1. To prevent a single person from having access to COMSEC material
2. To prevent more than two persons from having access to COMSEC material
3. To provide for an alternate custodian in the event the primary is unavailable
4. To allow for a division of responsibilities among the custodians

A. CRYPTO
B. Cryptoinformation
C. Crypto-related information
D. Cryptosystem

Figure 3C

IN ANSWERING QUESTIONS 3-36 THROUGH 3-39, SELECT THE TERM FROM FIGURE 3C THAT IS DESCRIBED.

3-36. Marking used to protect or authenticate national security-related information on all keying material and associated equipment.

1. A
2. B
3. C
4. D

3-37. Always classified and normally concerns the encryption or decryption process of a cryptosystem.

1. A
2. B
3. C
4. D

3-38. May be classified or unclassified; normally associated with cryptomaterial but not significantly descriptive of it.

1. A
2. B
3. C
4. D

3-39. Encompasses all associated items of cryptomaterial that provide a single means of encryption and decryption.

1. A
2. B
3. C
4. D

3-40. A failure that adversely affects the security of a cryptosystem is known by what term?

1. Cryptoexposure
2. Cryptoinstability
3. Cryptodeficiency
4. Cryptoinsecurity

3-41. A system within a general system confined to actual encryption, decryption, or authentication is known by what term?

1. Cryptovariable
2. Specific cryptosystem
3. Secondary cryptosystem
4. Supporting cryptosystem

3-42. The most frequently changed element of a cryptosystem is known by what term?

1. Primary cryptovariable
2. Secondary cryptovariable
3. Crypto modifier
4. Cryptosystem internal variable

3-43. What are the primary advantages of (a) over-the-air rekey (OTAR) and (b) over-the-air transfer (OTAT)?

1. (a) Requires less circuit downtime for loading keylists, and (b) no operator training required
2. (a) Reduces distribution of physical keying material, and (b) eliminates process of loading equipment with key tapes
3. (a) Reduces distribution of physical keying material, and (b) no operator training required
4. (a) Eliminates process of loading equipment with key tapes, and (b) no operator training required

3-44. What is the purpose of transmission authentication?

1. To guard against fraudulent or simulated transmissions
2. To inform the other operator that you are receiving the transmission
3. To acknowledge the transmission of the other operator
4. To allow the other operator to acknowledge your transmission

3-45. The self-authentication method is used in which of the following transmissions?

1. Transmission and reply
2. Challenge and reply
3. Transmission authentication
4. Challenge authentication

3-46. When you receive a message that has an authenticator in it, what action, if any, are you required to take?

1. Prepare a message to challenge the originator
2. Send a message that you are in receipt of the message
3. Pass the message on to higher authority for them to challenge the originator
4. None

3-47. As an operator, you are required to authenticate in which of the following situations?

1. You suspect intrusion on the circuit
2. You are requested to authenticate
3. You are requested to break radio silence
4. Each of the above

A. Meaconing
B. Interference
C. Jamming
D. Intrusion

Figure 3D

IN ANSWERING QUESTIONS 3-48 THROUGH 3-51, SELECT THE TERM FROM FIGURE 3D THAT IS DEFINED.

3-48. The interception and rebroadcast of navigational signals on the same frequency.

1. A
2. B
3. C
4. D

3-49. An attempt by the enemy to enter U.S. or allied communications systems and simulate traffic with the intent to confuse and deceive.

1. A
2. B
3. C
4. D

3-50. The deliberate use of electromagnetic signals with the objective of impairing communications circuits.

1. A
2. B
3. C
4. D

3-51. Usually a nondeliberate electrical disturbance that unintentionally prevents the effective use of a frequency.

1. A
2. B
3. C
4. D

3-52. Which of the following statements best describes the overall goal of AIS security?

1. To take all reasonable measures to protect AIS assets
2. To prevent data and programs from being destroyed or sabotaged
3. To keep unauthorized personnel out of your AIS facility
4. To take whatever measures are necessary to protect equipment and people

3-53. Which of the following assets is NOT considered an AIS asset?

1. People
2. Hardware
3. Software
4. Environment

3-54. In AIS security terminology, what term is used for the things that can destroy AIS assets?

1. Threats
2. Probability
3. Vulnerability
4. Countermeasures

3-55. To express the cost of a loss or abuse from an adverse event over time, what AIS security term is used?

1. Risk
2. Likelihood
3. Vulnerability
4. Countermeasure

3-56. In AIS security, risks are usually expressed in which of the following terms?

1. Days
2. Dollars
3. Equipment
4. Personnel

3-57. In AIS security terminology, the controls to lessen or eliminate known threats and vulnerabilities are called

1. physical barriers
2. security routines
3. backup procedures
4. countermeasures

3-58. Under AIS security, countermeasures (controls) that are embedded in hardware, software, and telecommunications equipment are what type of controls?

1. Physical
2. Technical
3. Managerial
4. Administrative

3-59. Under AIS security, countermeasures (controls) that concern people and procedures, such as who is authorized to do what or who receives or requests a sensitive report, are what type of controls?

1. Physical
2. Technical
3. Managerial
4. Administrative

3-60. Under AIS security, countermeasures (controls) that concern planning and evaluation, such as audits to review the effectiveness and efficiency of countermeasures that are in place, are what type of controls?

1. Physical
2. Technical
3. Managerial
4. Procedural

3-61. In regard to AIS security, the continuation of an activity's mission during abnormal operating conditions is provided by which of the following means?

1. Countermeasures
2. Contingency plans
3. Security risk plan
4. Emergency response team

3-62. In addition to hardware and software, what are the other three areas of consideration for the Navy's AIS security program?

1. Data, personnel, and environment
2. Data, human resources, and logistics
3. Data, human resources, and communications
4. Media libraries, environment, and communications

3-63. Which of the following personnel serves as the single point of contact for all matters related to AIS security?

1. Executive officer
2. Information system security manager
3. Security violations officer
4. Systems security manager

3-64. AIS security is not really that difficult to understand. What percent is (a) common sense, and (b) proper training?

1. (a) 55% (b) 45%
2. (a) 60% (b) 40%
3. (a) 65% (b) 35%
4. (a) 70% (b) 30%

3-65. The manufacturer's optimum temperature and humidity range specifications for AIS equipment operation are NOT available. Which of the following (a) temperature and (b) humidity ranges are considered acceptable for computer operation?

1. (a) 65° ±5° (b) 55% ±5%
2. (a) 65° ±5° (b) 65% ±2%
3. (a) 72° ±2° (b) 55% ±5%
4. (a) 72° ±2° (b) 65% ±2%

3-66. In AIS environmental security, emergency lights are installed in computer facilities for what primary reason?

1. To protect personnel
2. To assist fire fighters
3. To locate AIS equipment
4. To locate fire-fighting equipment

3-67. Fluctuations in electrical power can adversely affect the operation of AIS equipment. If your command's mission dictates continuous AIS support, each computer system should be equipped with which of the following equipment?

1. A motor/generator
2. An ac, dc regulator
3. A voltage surge protector
4. An uninterrupted power source

3-68. In regard to AIS security, master control switches are used to shut off all power to your AIS spaces in the event of a fire. These master control switches are normally installed at what location?

1. In the $CO^2$ storage room
2. In the security officer's space
3. At the exit doors of the AIS spaces
4. On the master control panel of the computer

3-69. Which of the following security modes does NOT apply to processing classified or level I data?

1. Dedicated
2. System low
3. Multilevel
4. System high

3-70. For processing classified, the central computer facility and all its related peripheral devices (both local and remote) are protected for the highest classification category and type of material contained in the system. The system is said to be in what security mode?

1. Controlled
2. System low
3. System high
4. Totally dedicated

3-71. For processing level I data, the central computer facility and all its related peripheral devices (both local and remote) are exclusively used and controlled by specific users having a security clearance and need-to-know for the processing of a particular cateqory of classified material. The system is operating in what security mode?

1. Dedicated
2. System low
3. Multilevel
4. System high

3-72. For processing level I data, an AIS system provides the capability of permitting various categories of classified materials to be stored, processed, and selectively accessed on a concurrent basis by users having differing clearances and need-to-know. The system is said to be in what security mode?

1. Controlled
2. Undedicated
3. System low
4. Multilevel

3-73. What category of AIS media is considered temporary in nature and is retained for 180 days or less?

1. Smooth
2. Working
3. Finished
4. Intermediate

3-74. Which of the following categories of AIS media is permanent in nature and is retained for a period of more than 180 days?

1. Smooth
2. Working
3. Finished
4. Intermediate

# ASSIGNMENT 4

Textbook Assignment: "AIS Security (continued)," chapter 4, pages 4-13 through 4-26.

---

4-1. In which of the following steps in planning an AIS security program, will major problem areas be identified?

1. Perform action plans
2. Perform preliminary planning
3. Perform a preliminary risk analysis
4. Perform and document a detailed risk analysis

4-2. Which of the following steps in planning an AIS security program allows for review and approval?

1. Perform action plans
2. Perform preliminary planning
3. Perform a preliminary risk analysis
4. Perform and document a detailed risk analysis

4-3. A security policy statement should provide which of the following information?

1. General guidance and assignment of responsibilities
2. General guidance and listing of responsibilities
3. Detailed guidance and assignment of responsibilities
4. Detailed guidance and listing of responsibilities

4-4. As a guideline for risk analysis, which of the following FIPS publications should you use?

1. FIPS PUB 47
2. FIPS PUB 53
3. FIPS PUB 65
4. FIPS PUB 79

4-5. The impact of a given threat may depend on all but which of the following factors?

1. Geographical location
2. Local environment
3. Perceived threat of vandals
4. Potential value of property to a thief

4-6. Which of the following is a threat to an AIS facility?

1. Hardware failure
2. Tampering with inputs, programs, and data
3. Accidents causing nonavailability of key personnel
4. Each of the above

4-7. It is recommended that the AIS facility upper management begin development of the security program with a/an

1. risk analysis
2. inventory of equipment
3. survey of data integrity
4. intensive training program

4-8. A quantitative risk analysis produces which of the following results?

1. Long-range planners receiving guidance on personnel requirements
2. The security program objectives directly relating to the mission of the command
3. Criteria generated for designing and evaluating internal controls
4. An estimate of losses to be expected

4-9. When the risk analysis is prepared, the first step to be considered is to

1. develop an estimate of annual loss expectancy
2. estimate the potential losses to which the AIS facility is exposed
3. evaluate the threats to the AIS facility
4. review the security program objectives

4-10. The loss potential estimate has which of the following objectives?

1. To place a monetary value on the loss estimate only
2. To identify critical aspects of the AIS facility operation only
3. To place a monetary value on the loss estimate and to identify critical aspects of the AIS facility operation
4. To determine data replacement requirements

4-11. The loss of program files has which of the following loss potentials?

1. Cost to replace assets
2. Cost to reconstruct files
3. Security compromise
4. Value of assets stolen before loss is detected

4-12. Which of the following is the loss potential that may result from the indirect theft of assets?

1. Cost to replace assets
2. Cost to reconstruct files
3. Security compromise
4. Value of assets stolen before loss is detected

4-13. To show replacement costs for the physical assets of the AIS facility, AIS technical managers and upper management should use which of the following methods?

1. Build a graph
2. Construct a table
3. Produce a list
4. Write a description

4-14. The AIS technical manager should call on which of the fallowing personnel to assist in making loss estimates?

1. Users
2. Vendors
3. Programmers
4. Supervisors

4-15. After a preliminary screening to identify the critical tasks, the AIS technical manager should perform which of the following tasks next?

1. Determine the scope of the critical tasks
2. Develop an estimate of annual loss expectancy
3. Quantify loss potential with the help of user representatives
4. Determine the back-up system requirements for the critical tasks

4-16. The second step to be considered when you prepare the risk analysis is to

1. develop an estimate of annual loss expectancy
2. estimate the potential losses to which the AIS facility is exposed
3. evaluate the threats to the AIS facility
4. review the security program objectives

4-17. To develop estimates of the occurrence probability for each type of threat, the AIS technical manager should use all except which of the following resources?

1. Standardized Navy-wide formula
2. Higher authority instructions/manuals
3. Common sense
4. Data

4-18. The third step to be considered when you prepare the risk analysis is to

1. develop an estimate of annual loss expectancy
2. estimate the potential losses to which the AIS facility is exposed
3. evaluate the threats to the AIS facility
4. review the security program objectives

4-19. Fire, flood, and sabotage, in varying degrees, result in which of the following losses?

1. Indirect loss of assets
2. Physical destruction
3. Data compromise
4. Theft of information

4-20. Reducing the probability of some occurrence by altering the environment could be accomplished in which of the following ways?

1. Implementing more rigorous standards for programming and software testing
2. Preparing a backup system for offsite operations
3. Providing military guards and special door locks
4. Relocating the AIS facility

4-21 Which of the following is an example of erecting barriers to ward off a threat?

1. Implementing more rigorous standards for programming and software testing
2. Preparing a backup system for offsite operations
3. Providing military guards and special door locks
4. Relocating the AIS facility

4-22. When selecting a specific remedial measure, a total of how many criteria should be used?

1. One
2. Two
3. Three
4. Four

4-23. Which of the following is one possible way to select a remedial measure to minimize a threat?

1. Begin with the threat having the largest annual loss potential
2. Begin with only those measures for which the cost can be estimated precisely
3. Begin with only those remedial measures that would not cause a loss reduction in the same area
4. Begin with the remedial measures for which the annual cost is more than the expected reduction in annual loss

4-24. All but which of the following events tends to have the same basic effect as the others on AIS operations?

1. Fire
2. Rain
3. Earthquake
4. Windstorm

4-25. In minimizing an AIS building's exposure to fire damage, which of the following factors should be considered?

1. Contractors
2. Design only
3. Location only
4. Design and location

4-26. An AIS physical security program should include which of the following fire safety elements?

1. Measures to ensure prompt detection of and response to a fire emergency
2. Provision for quick human intervention and adequate means to extinguish fires
3. Provision of adequate means and personnel to limit damage and effect prompt recovery
4. All of the above

4-27. In evaluating the fire safety of an AIS facility, a total of how many factors are to be considered?

1. Five
2. Six
3. Three
4. Four

4-28. Which of the following factors affects the degree of hazard associated with a given occupancy?

1. Weight of the material
2. Amount of combustible material
3. Exposed surface of the material
4. Package in which the material is stored

4-29. When the safety features of an AIS facility building are designed, which of the following factors should be considered?

1. Heat-resistant lights
2. Building operation
3. Fire walls
4. Storm doors

4-30. The inherent fire safety of a building can be rendered ineffective because of which of the following conditions?

1. Fire doors propped open
2. Standard electrical wiring
3. Use of low-flame spread materials
4. Products-of-combustion detectors

4-31. Experience in fire fighting shows that the major factor in limiting fire damage is

1. prompt detection of fires
2. experienced fire fighters
3. multiple fire extinguishers
4. quick response time to alarms

4-32. During the third stage of a fire, fire fighting becomes increasingly difficult and often people cannot remain at the fire site for which of the following reasons?

1. Toxic gases only
2. High temperatures only
3. Large volume of smoke only
4. Toxic gases, high temperatures, and large volume of smoke

4-33. Prompt fire detection is best accomplished through the use of which of the following detectors?

1. Gas
2. Heat
3. Smoke
4. Flame

4-34. When detectors are installed, which of the following factors need NOT be considered?

1. The location of equipment
2. The direction and velocity of air flow
3. The presence of areas with stagnant air
4. The location of fire extinguishers

4-35. In the design of the detection control panel, which of the following indications should be included?

1. The power supply status of each detector
2. Which detector has alarmed
3. The cause of the alarm
4. What type of detector has alarmed

4-36. To assure that someone will be alerted to a fire, which of the following alarm locations is recommended as the primary location?

1. Computer room
2. Personnel office
3. Commanding officer's office
4. Buildinq maintenance

4-37. Reducing the sensitivity of the smoke detectors to eliminate nuisance alarms may have which of the following results?

1. Save energy
2. Extend equipment life
3. Delay fire detection
4. Cause poor personnel performance

4-38. In an actual fire situation, the air handling equipment could be shut down automatically to avoid which of the following problems?

1. Straining the air handling equipment
2. Excessive energy consumption
3. Excessive filter wear
4. Spreading smoke and fanning the flames

4-39. When fire detection systems are interconnected with air handling equipment, a preferred technique is to cause the system to take which of the following measures?

1. Exhaust the smoke
2. Lower the thermostat
3. Recirculate the smoke
4. Use inside air for intake

4-40. What is the minimum temperature required to activate an automatic sprinkler system?

1. 115°F
2. 125°F
3. 135°F
4. 145°F

4-41. To ensure the effectiveness of portable extinguishers, which of the following measures should be observed?

1. Extinguishers should be marked for rapid identification
2. Extinguishers should have inspection tags
3. Extinguishers should be placed in corners
4. Extinguishers should be placed on the floor, not mounted

4-42. Military personnel who are knowledgeable and trained in fire safety are needed by which of the following types of commands?

1. Small commands only
2. Medium commands only
3. Large commands only
4. Every command

4-43. When using supporting utilities, AIS technical managers should consider the probability of occurrence and the effects of which of the following conditions?

1. Vandalism only
2. Sabotage only
3. Fire only
4. Vandalism, sabotage, and fire

4-44. Excessive fluctuation in the dc voltage applied to the hardware can be caused if the line voltage is 90 percent or less of nominal for more than what minimum number of milliseconds?

1. 7
2. 6
3. 5
4. 4

4-45. Power fluctuations in line voltage cause unpredictable results in which of the following components?

1. Logic only
2. Hardware only
3. Data transfer only
4. Logic, hardware, and data transfer

4-46. In an AIS facility, the effects of internal power fluctuations can be minimized in which of the following ways?

1. Grounding the CPU
2. Isolating the AIS hardware from other facility loads
3. Wiring all components in parallel
4. Wiring each component with a circuit breaker

4-47. The technique of connecting the AIS facility to more than one utility feeder has more protection value when the feeders are connected in what manner?

1. To the same junction box
2. From the same utility pole
3. To different power substations
4. To different utility meters

4-48. An uninterrupted power supply (UPS) consists of a solid-state rectifier that performs which of the following functions?

1. Drives a solid-state inverter only
2. Keeps batteries charged only
3. Drives a solid-state inverter and keeps batteries charged
4. Synthesizes alternating current

4-49. The UPS battery supply can support a facility load for a maximum of how many minutes?

1. 35
2. 40
3. 45
4. 50

4-50. The control circuitry for a static transfer switch performs which of the following functions?

1. Senses variations in frequency
2. Senses an overcurrent condition
3. Switches the load to the alternate power source
4. Stops the flow of power

4-51. Using multiple, independent UPS units can provide which of the following benefits?

1. Power consumption is lowered
2. Each unit can be switched offline if it fails
3. The metering of component power consumption is facilitated
4. All of the above

4-52. If the risk analysis shows a major loss from power outages lasting 30 to 45 minutes or longer, which of the following measures should be taken?

1. Installing an on-site generator
2. Cutting back on operations
3. Relocating the facility
4. Adding more multiple, independent UPS units

4-53. Which of the following components must be large enough to support air-conditioning or minimum lighting as well as the UPS load?

1. Generator
2. Alternator
3. Prime mover
4. Alternate mover

4-54. Providing physical protection for an AIS facility involves which of the following processes?

1. Denying access to unauthorized persons
2. Permitting access to authorized persons
3. Both 1 and 2 above
4. Minimizing the risks of a natural disaster

4-55. Wherever AIS equipment is used for processing classified information, which of the following instructions should be used for applying physical protection and security policy?

1. OPNAVINST 5230.12
2. OPNAVINST 5239.1
3. SECNAVINST 5211.5
4. SECNAVINST 5233.1

4-56. Which of the following contingency plans for dealing with classified material should NOT be considered in emergencies?

1. Destruction
2. Protection
3. Removal
4. Reproduction

4-57. In an emergency, the placement of a perimeter guard force around the affected area provides protection in which of the following ways?

1. Provides external contact when communications are lost
2. Prevents the removal of classified material
3. Reduces the risk of additional destruction
4. Provides AIS access control

4-58. Which of the following methods may be used to protect the property boundary of the AIS facility?

1. Roving patrol only
2. Fencing-only
3. Roving patrol and fencing
4. Security badges

4-59. Fences installed for boundary protection should be (a) what minimum height with (b) what minimum number of strands of barbed wire?

1. (a) 8 feet (b) 2
2. (a) 8 feet (b) 3
3. (a) 10 feet (b) 2
4. (a) 10 feet (b) 3

4-60. Penetration sensors mounted on fences and gates should provide which of the following alarms when tripped?

1. External only
2. Internal only
3. External and internal

4-61. Tests show that electromagnetic or acoustic emanations from AIS hardware. may be intercepted up to a maximum of how many yards away?

1. 150
2. 230
3. 325
4. 400

4-62. If the AIS technical manager plans to take measures to control compromising emanations, those measures are subject to approval under the provisions of which of the following DOD directives?

1. 5200.19
2. C5200.19
3. 5200.28
4. C5200.28

4-63. The application of the measures to control compromising emanations within the industrial AIS systems is at the direction of the contracting activity concerned under the provisions of which of the following DOD directives?

1. 5200.19
2. C5200.19
3. 5200.28
4. C5200.28

4-64. The use of an intrusion detection system (IDS) in a protective program is covered in which of the following instructions?

1. OPNAVINST 5239.1
2. OPNAVINST 5510.1
3. SECNAVINST 5211.5
4. SECNAVINST 5233.1

4-65. The physical security requirements for a remote terminal area are based upon which of the following classifications?

1. The classification of the central computer facility
2. The classification of the remote terminal area
3. The classification of the data that will be accessed through the terminal
4. The classification assigned by higher authority

4-66. When the AIS system contains classified information, what action, if any, must be taken for each remote terminal that is not controlled?

1. Disconnect
2. Place offline
3. Turn off
4. None

4-67. In the annual security survey of an AIS facility, what is the second step?

1. Define and tabulate areas within the facility for control purposes
2. Evaluate all potential threats to the AIS facility
3. Identify areas where remedial measures are needed
4. Recommend improvements to upper management

4-68. When the annual security survey is conducted, it should begin at which of the following areas?

1. Roof
2. Basement
3. Perimeter
4. Top floor

4-69. When surveying the perimeter of the facility, the AIS technical manager need NOT check which of the following accessways?

1. Fire escapes
2. Doors and windows
3. Other entrances, such as vents
4. Manned posts at the property line

4-70. When surveying the internal security of a facility, the AIS technical manager should follow which of the following guidelines?

1. Begin the survey on the roof
2. Determine where alarms annunciate
3. Finish the survey in the mailroom area
4. Note the volume of the alarms

IN ANSWERING QUESTION 4-71, REFER TO TABLE 4-6 IN THE TEXT.

4-71. Which of the following questions need NOT be included in the physical security survey?

1. Is the present equipment up-to-date?
2. Is the alarm system inspected and tested occasionally to ensure operation?
3. What kind of sound does the alarm make?
4. How many zones of protection are within the protected building?

4-72. Which of the following facts are used by the AIS technical manager to evaluate existing access controls and protection measures?

1. The schedule of alarm tests
2. The design of the alarm system
3. The number and location of manned posts
4. The distance between the manned posts and the building

4-73. Which of the following items are prepared and executed for the accomplishment of the command’s specific mission?

1. Operation plans only
2. Operation plans and-the command’s organizational manual
3. Emergency response plans only
4. Emergency response plans and the command’s organizational manual

4-74. A total of how many different types of contingency plans make up a COOP security plan?

1. One
2. Two
3. Three
4. Four

4-75. The risk analysis should be reviewed by which of the following people?

1. Production control clerk
2. Response team
3. Technical manager
4. Upper management

# ASSIGNMENT 5

Textbook Assignment: "AIS Security (continued)," chapter 4, pages 4-26 through 4-40; "General Security," chapter 5, pages 5-1 through 5-13.

---

5-1. The AIS technical manager can develop measures to use in case of emergency by reviewing operations and records with which of the following personnel?

1. Production control clerk
2. Response team members
3. Shift leaders
4. Users

5-2. All personnel should be instructed to take which of the following security measures if an evacuation of work areas is ordered?

1. Secure classified material in desks or file cabinets
2. Turn equipment and room lights off
3. Close the doors as areas are evacuated but leave the doors unlocked
4. Power up the air-conditioning equipment

5-3. To ensure that all safety requirements of the AIS facility are satisfied, the AIS technical manager and the operations division officer should review the protective plans with what frequency?

1. Monthly
2. Quarterly
3. Semiannually
4. Annually

5-4. Backup operations may take place onsite under which of the following conditions?

1. A partial loss of capability
2. Major damage only
3. Major destruction only
4. Major damaqe and destruction

5-5. For the purpose of making backup resources available, which of the following tasks can be set aside?

1. Short-term planning
2. Program development
3. Weekly processing
4. Backup processing

5-6. When backup alternatives are considered, which of the following substitute procedures may be implemented during an emergency?

1. A hard disk input could be used for a failed telephone input
2. Online processing could be substituted for batch processing
3. Print tapes could be carried to a backup facility for offline printing
4. Both 2 and 3 above

5-7. To evaluate alternate backup modes and offsite facilities, you should consider all but which of the following factors?

1. AIS hardware usage
2. Maintenance personnel for your AIS building
3. Overtime cost factor for civil service personnel
4. Transportation of personnel with needed supplies and materials

5-8. When developing the optimum backup plan, it is wise to form several backup plans, one of which has which of the following charac-teristics?

1. Extends beyond the cause of delay
2. Includes each minor partial failure
3. Lasts at least half the time required to reconstruct the facility
4. Includes one or more operating periods between minimum duration and worst case

5-9. Each COOP backup plan should cover a total of how many basic areas?

1. Five
2. Six
3. Three
4. Four

A. Administrative information
B. Computer system specifications
C. Performance specifications
D. User instructions

Figure 5A

IN ANSWERING QUESTIONS 5-10 THROUGH 5-12, SELECT FROM FIGURE 5A THE AREA OF THE COOP BACKUP PLAN DESCRIBED.

5-10. The specific ways in which performance of each task departs from normal is stated.

1. A
2. B
3. C
4. D

5-11. Input in different forms may be required.

1. A
2. B
3. C
4. D

5-12. The location of the system is given.

1. A
2. B
3. C
4. D

5-13. The process of recovery will be carried out more effectively and economically if handled by which of the following personnel?

1. The users only
2. The AIS staff only
3. The users and AIS staff
4. Personnel other than the AIS staff

5-14. Before recovery from total destruction is achieved, all but which of the following tasks must be completed?

1. Locating floor space for the AIS facility without regard for live load capacity
2. Verifying all needed hardware, equipment, and materials
3. Performing facility modifications
4. Procuring hardware

5-15. For COOP testing, a team should be assembled to perform all except which of the following tasks?

1. Prepare a scenario for the test
2. Control and observe the test
3. Evaluate the test results
4. Provide training

5-16. Which of the following is a standard for an AIS facility inspection?

1. It should be dependent and subjective
2. It should examine the information system and its use
3. It should ignore adequacy controls
4. It should be the first element in a physical security program

5-17. The characteristic of an inspection being independent and objective implies that the inspection has which of the following relationships to management?

1. Replaces normal management inspections
2. Is a part of normal management visibility
3. Complements normal management inspections
4. Is a substitute for the management reporting, system

5-18. An inspection can be expected to accomplish which of the following tasks?

1. Evaluate security controls for the AIS facility
2. Provide users an opportunity to maintain the AIS security program
3. Provide the impetus to keep workers and management complacent
4. Uncover adequate operational areas

5-19. In determining the frequency of internal inspections, the AIS technical manager should consider which of the followinq factors?

1. Operation workload
2. The rate of change of the AIS
3. The SOPS of the AIS staff
4. The results of the last inspection only

5-20. What is the role of the inspection team?

1. To develop security controls
2. To evaluate established controls
3. To enforce control procedures
4. To develop security procedures

5-21. Which of the following characteristics of the inspection board members will NOT affect the success of the inspection?

1. Ability
2. Objectivity
3. Probing nature
4. Punctuality

5-22. Which of the following is NOT an important characteristic for the inspection board members?

1. Ability to enforce controls
2. Attention to detail
3. Inquisitiveness
4. Probing nature

5-23. Which of the following types of expertise is helpful for a member of the inspection team?

1. Operations experience only
2. Security experience only
3. Security experience and programming knowledge
4. Operations experience and programming knowledge

5-24. The group of people who have the most to gain from an effective inspection are the

1. members of the inspection team
2. members of the security force
3. programmers in the facility
4. users of the facility

5-25. Which of the following is a characteristic of a comprehensive inspection plan?

1. It is action-oriented
2. It lists actions to be bypassed
3. It is tailored for universal installation
4. It allows freedom in the report design

5-26. In developing a comprehensive inspection plan, what is the third step?

1. Review the risk analysis plan
2. Examine the security policy and extract pertinent objectives
3. Examine the AIS facility organization chart and job descriptions
4. Review documents to determine the specified security operating procedures

5-27. When formulating the inspection program, which of the following areas is the most important to consider?

1. The most recent security breach without regard for security priorities
2. The activities that produce minimum results with the most effort
3. The critical issues with regard to security
4. The measures that are tested most frequently in day-to-day operations

5-28. It is considered advantageous to test fire detection sensors under surprise conditions for which of the following reasons?

1. To test the response to alarms
2. To test the reaction of the fire party
3. To test the effectiveness of evacuation plans
4. Each of the above

5-29. Why should the review of previous inspection reports be part of the process of developing an inspection plan?

1. To show trends
2. To identify weaknesses that should have been corrected
3. To identify strengths that were identified
4. To identify previous team members

5-30. With what frequency should a scheduled inspection take place?

1. Monthly
2. Quarterly
3. Semiannually
4. Annually

5-31. A surprise inspection should be approved by which of the following personnel?

1. The facility security officer
2. The AIS technical manager
3. The commanding officer of the command in charge of the AIS facility
4. The commanding officer of the user command

5-32. In conducting a scheduled inspection, which of the following is normally the first step?

1. Interviewing the AIS personnel
2. Scrutinizing the AIS facility records
3. Inventorying the AIS hardware capabilities of the facility
4. Testing the AIS facility access control procedures

5-33. Most security inspections include testing which of the following activities at AIS facilities?

1. Fire-fighting procedures
2. Facility evacuation
3. System backup
4. Personnel placement procedures

5-34. What is the preferred frequency at which the inspection team should convene to review progress and compare notes?

1. At the end of each day’s activity
2. At the end of each week’s activities
3. Every 2 weeks
4. Every 3 weeks

5-35. After the completion of the inspection, when should the written report be prepared?

1. When requested by the supervisor of the AIS facility being inspected
2. When requested by the commanding officer of the AIS facility being inspected
3. Immediately after the inspection, while the impressions are still fresh
4. After an extended period of time to allow the inspection team members to reflect on the inspection process

5-36. Who is responsible for implementing the recommendations received from the inspection?

1. The AIS technical manager
2. The security officer
3. The commanding officer
4. The TYCOM

5-37. The best approach in assigning responsibilities for corrective action is to summarize each major deficiency on a control sheet outlining which of the following areas?

1. An executive summary
2. The action taken or required
3. The date the deficiency was discovered
4. The reporting official

5-38. For any control item that is still open, it is recommended that reports be turned in to upper management with what frequency?

1. Weekly
2. Monthly
3. Quarterly
4. Semiannually

5-39. Which of the following instructions provides guidelines for implementing security safeguards required to implement the Privacy Act of 1974?

1. SECNAVINST 5211.5
2. SECNAVINST 5239.2
3. OPNAVINST 5510.1
4. OPNAVINST 5239.1

5-40. Which of the following subsections of the Privacy Act (title 5, section 552a) requires the use of safeguards to ensure the confidentiality and security of records?

1. Subsection (b)
2. Subsection (c)
3. Subsection (e) (5)
4. Subsection (e) (10)

5-41. A personal data security risk assessment benefits a command in all but which of the following ways?

1. It saves money that might have been wasted on safeguards that do not significantly lower the overall data risks
2. It ensures that additional security safeguards help to counter all the serious personal data security risks
3. It provides a basis for deciding whether additional security safeguards are needed for personal data
4. It considers only the risks to personal data

5-42 . Which of the following participants should NOT be included on the risk assessment team?

1. A representative of the operating facility
2. An individual responsible for security
3. A system programmer
4. A systems analyst

5-43. Data may be misrouted, mis-labeled, or it may contain unexpected personal information as a result of which of the following data security risks?

1. Input errors
2. Program errors
3. Improper data dissemination
4. Mistaken processing of data

5-44. When security measures to adequately control system access to personal data are developed, they should include protection from all except which of the following risks?

1. Dial-in access
2. Open system access
3. Physical destruction of the AIS
4. Unprotected files and theft of data

5-45. Commands designing large computer networks should consider which of the following risks early in the planning stages?

1. Eavesdropping only
2. Misidentified access and eavesdropping only
3. Operating system flaws and subverting programs only
4. Misidentified access, eavesdropping, operating systems flaws, subverting programs, and spoofing

5-46. Information management practices include all but which of the following activities?

1. Data collection, validation, and transformation
2. Information processing or handling
3. Information control, display, and presentation
4. Managerial determination of the need and use of the information

5-47. Which of the following practices is/are suggested for the handling of personal data?

1. Label recording media that contain data of local personnel only
2. Carefully control products of intermediate processing steps
3. Maintain an online, up-to-date hardcopy authorization list of all individuals who have access to any data
4. Both 2 and 3 above

5-48. Which of the following practices is/are suggested for the maintenance of personal records?

1. Establish procedures for maintaining correct, current accounting of all new personal data brought into the computer facility
2. Maintain logbooks for terminals that are used to access any data by system users
3. Both 1 and 2 above
4. Log each transfer of storage media containing data to the computer facility

5-49. For a broader knowledge of personal identification and identification techniques, you should refer to which of the FIPS publications?

1. FIPS PUB 31
2. FIPS PUB 48
3. FIPS PUB 79
4. FIPS PUB 114

5-50. Which of the following pieces of equipment might be considered a TEMPEST hazard?

1. Personal computer
2. Electric typewriter
3. Both 1 and 2 above
4. A copying machine

5-51. The vulnerability of a ship or aircraft can be determined by which of the following means?

1. A TEMPEST survey
2. A TEMPEST vulnerability assessment
3. A TEMPEST investigation
4. An emission control test

5-52. What is the purpose of EMCON?

1. To intercept and rebroadcast signals to confuse hostile forces
2. To prevent hostile forces from detecting, identifying, and locating friendly forces
3. To minimize the amount of transmission time on live circuits
4. Both 2 and 3 above

4-53. What is the designation of security spaces requiring access control?

1. Controlled area
2. Exclusion area
3. Restricted area
4. Limited area

4-54. Which of the following information should appear in a visitors log for a communications center?

1. Visitor’s printed name and signature
2. Purpose of visit and the escort’s name
3. Date and time of visit
4. Each of the above

5-55. The combination to a classified material container must be changed at what maximum interval?

1. Monthly
2. Every 6 months
3. Every 12 months
4. Every 24 months

5-56. Which of the following statements concerning the security classification of a safe combination is correct?

1. All combinations are classified Secret regardless of the classification of contents stored within
2. All combinations are classified Confidential regardless of the classification of contents stored within
3. All combinations are handled as official information
4. Combinations are assigned a security classification equal to the highest category of classified material stored

5-57. An individual who is responsible for safeguarding and accounting for classified material is known by what term?

1. Custodian
2. User
3. Keeper
4. Guardian

5-58. Which of the following conditions for protecting classified material after workinq hours is NOT in accordance with security instructions?

1. Classified documents are in locked authorized containers
2. Classified notes, carbon paper, typewriter ribbons, and rough drafts have been destroyed or are in locked authorized containers
3. The contents of wastebaskets containing classified material were not burned, but are in locked authorized containers
4. Burn bags, ready for burning the next day, are securely stapled, numbered, and neatly lined up along the bulkhead

5-59. What is the minimum number of times the dial of a security container must be rotated in the same direction to ensure it is locked?

1. Five
2. Two
3. Three
4. Four

5-60. During routine destruction of classified material, what is the ultimate goal of the destruction?

1. To clear files of old material so there is more room for new material
2. To make reconstruction of the material impossible
3. To prevent unauthorized reproduction
4. To destroy the material as quickly as possible

5-61. What is the most efficient means of destroying classified material?

1. Burning
2. Shredding
3. Jettisoning
4. Pulping

5-62. Persons witnessing destruction of classified material must have a security clearance of at least what level?

1. Confidential
2. Secret
3. Top Secret
4. The level of the material being destroyed

5-63. When is a record of destruction required for Secret messages?

1. If only one person performs destruction
2. If the messages have special markings
3. If the messages have to be jettisoned
4. During routine destruction

5-64. Records of destruction of classified material must be maintained for what minimum length of time?

1. 1 yr
2. 2 yr
3. 6 mo
4. 18 mo

5-65. How are burn bags accounted for prior to burning?

1. Bags are placed in a secure place and inventoried daily
2. Each bag must be serially numbered and a record kept of all subsequent handling until destroyed
3. Each office is responsible for its burn bag until the day of destruction
4. On the day of destruction, each bag is serially numbered

5-66. What is the maximum allowable size of material shredded by a crosscut shredding machine?

1. 1/32 inch wide by 1 inch long
2. 1/32 inch wide by 1/2 inch long
3. 3/64 inch wide by 1/2 inch long
4. 3/64 inch wide by 1 inch long

5-67. If classified material must be jettisoned during emergency destruction, what should be the minimum depth of the water?

1. 500 fathoms
2. 700 fathoms
3. 1,000 fathoms
4. 5,000 fathoms

5-68. Which of the following areas must be covered in a command's emergency action plan?

1. Enemy actions
2. Civil disturbances
3. Natural disasters
4. Each of the above

5-69. When a command implements its emergency plan, the priority of destruction should be based on what factor?

1. The speed at which the material can be destroyed
2. The amount of material that can be destroyed in the least amount of time
3. The potential effect on national security should the material fall into hostile hands
4. The number of personnel required for destruction

5-70. When an emergency plan is implemented, which of the following material should be destroyed first?

1. SPECAT material
2. Special access material
3. COMSEC material
4. PERSONAL FOR material

5-71. In addition to having an emergency destruction plan, all commands are required to have what other type of emergency plan?

1. Fire
2. Evacuation
3. Security force
4. Watch security

5-72. Which of the following material should NOT be destroyed during a precautionary destruction?

1. Material of a historical nature
2. Material that has been superseded
3. Material essential to communications
4. Material that is unneeded

5-73. What should be done with superseded classified material?

1. Retain indefinitely
2. Retain for two years, then destroy
3. Retain for one month, then destroy
4. Destroy in accordance with its prescribed time frame

STUDENT COMMENT SHEET

THIS FORM MAY BE USED TO SUGGEST IMPROVEMENTS, REPORT COURSE ERRORS, OR TO REQUEST HELP IF YOU HAVE DIFFICULTY COMPLETING THE COURSE.

**NOTE: IF YOU HAVE NO COMMENTS, YOU DO NOT HAVE TO SUBMIT THIS FORM.**

Date_____

FROM:

_____
RATE/RANK/GRADE, NAME (FIRST, M.I., LAST)

DSN:_____
_____ Commercial:_____
STREET ADDRESS, APT # FAX:_____
INTERNET:_____

_____
CITY, STATE, ZIP CODE

To. COMMANDING OFFICER
NETPDTC CODE N311
6490 SAUFLEY FIELD RD
PENSACOLA FL 32509-5237

Subj: RADIOMAN TRAINING SERIES, MODULE 1- ADMINISTRATION AND SECURITY, NAVEDTRA 12845

1. The following comments are hereby submitted:

PRIVACY ACT STATEMENT

UNDER AUTHORITY OF TITLE 5, USC 301, INFORMATION REGARDING YOUR MILITARY STATUS IS REQUESTED TO ASSIST IN PROCESSING YOUR COMMENTS AND IN PREPARING A REPLY. THIS INFORMATION WILL NOT BE DIVULGED WITHOUT WRITTEN AUTHORIZATION TO ANYONE OTHER THAN THOSE WITHIN DOD FOR OFFICIAL USE IN DETERMINING PERFORMANCE.

. . . . . (Fold along dotted line . . . . . .

. . . . . (Fold along dotted fine) . . . . . .

**DEPARTMENT OF THE NAVY**

**COMMANDING OFFICER**
**NETPDTC CODE N311**
**6490 SAUFLEY FIELD RD**
**PENSACOLA FL 32509-5237**

**OFFICIAL BUSINESS**

**COMMANDING OFFICER**
**NETPDTC CODE N311**
**6490 SAUFLEY FIELD RD**
**PENSACOLA FL 32509-5237**

NAVEDTRA 1430/5
Stock Ordering No. 0502-LP-216-0100

PRINT OR TYPE

TITLE_____ NAVEDTRA_____

NAME_____ ADDRESS_____
Last First Middle Street/Ship/Unit/Division, etc.

_____
City or FPO State Zip

RANK/RATE_____ SSN_____ DESIGNATOR_____ ASSIGNMENT NO._____ DATE SUBMITTED _____

☐ USN ☐ USNR ☐ ACTIVE ☐ INACTIVE OTHER (Specify)_____

SCORE

| | 1 T | 2 F | 3 | 4 | | | 1 T | 2 F | 3 | 4 | | | 1 T | 2 F | 3 | 4 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ☐ | ☐ | ☐ | ☐ | _____ | 26 | ☐ | ☐ | ☐ | ☐ | _____ | 51 | ☐ | ☐ | ☐ | ☐ | _____ |
| 2 | ☐ | ☐ | ☐ | ☐ | _____ | 27 | ☐ | ☐ | ☐ | ☐ | _____ | 52 | ☐ | ☐ | ☐ | ☐ | _____ |
| 3 | ☐ | ☐ | ☐ | ☐ | _____ | 28 | ☐ | ☐ | ☐ | ☐ | _____ | 53 | ☐ | ☐ | ☐ | ☐ | _____ |
| 4 | ☐ | ☐ | ☐ | ☐ | _____ | 29 | ☐ | ☐ | ☐ | ☐ | _____ | 54 | ☐ | ☐ | ☐ | ☐ | _____ |
| 5 | ☐ | ☐ | ☐ | ☐ | _____ | 30 | ☐ | ☐ | ☐ | ☐ | _____ | 55 | ☐ | ☐ | ☐ | ☐ | _____ |
| 6 | ☐ | ☐ | ☐ | ☐ | _____ | 31 | ☐ | ☐ | ☐ | ☐ | _____ | 56 | ☐ | ☐ | ☐ | ☐ | _____ |
| 7 | ☐ | ☐ | ☐ | ☐ | _____ | 32 | ☐ | ☐ | ☐ | ☐ | _____ | 57 | ☐ | ☐ | ☐ | ☐ | _____ |
| 8 | ☐ | ☐ | ☐ | ☐ | _____ | 33 | ☐ | ☐ | ☐ | ☐ | _____ | 58 | ☐ | ☐ | ☐ | ☐ | _____ |
| 9 | ☐ | ☐ | ☐ | ☐ | _____ | 34 | ☐ | ☐ | ☐ | ☐ | _____ | 59 | ☐ | ☐ | ☐ | ☐ | _____ |
| 10 | ☐ | ☐ | ☐ | ☐ | _____ | 35 | ☐ | ☐ | ☐ | ☐ | _____ | 60 | ☐ | ☐ | ☐ | ☐ | _____ |
| 11 | ☐ | ☐ | ☐ | ☐ | _____ | 36 | ☐ | ☐ | ☐ | ☐ | _____ | 61 | ☐ | ☐ | ☐ | ☐ | _____ |
| 12 | ☐ | ☐ | ☐ | ☐ | _____ | 37 | ☐ | ☐ | ☐ | ☐ | _____ | 62 | ☐ | ☐ | ☐ | ☐ | _____ |
| 13 | ☐ | ☐ | ☐ | ☐ | _____ | 38 | ☐ | ☐ | ☐ | ☐ | _____ | 63 | ☐ | ☐ | ☐ | ☐ | _____ |
| 14 | ☐ | ☐ | ☐ | ☐ | _____ | 39 | ☐ | ☐ | ☐ | ☐ | _____ | 64 | ☐ | ☐ | ☐ | ☐ | _____ |
| 15 | ☐ | ☐ | ☐ | ☐ | _____ | 40 | ☐ | ☐ | ☐ | ☐ | _____ | 65 | ☐ | ☐ | ☐ | ☐ | _____ |
| 16 | ☐ | ☐ | ☐ | ☐ | _____ | 41 | ☐ | ☐ | ☐ | ☐ | _____ | 66 | ☐ | ☐ | ☐ | ☐ | _____ |
| 17 | ☐ | ☐ | ☐ | ☐ | _____ | 42 | ☐ | ☐ | ☐ | ☐ | _____ | 67 | ☐ | ☐ | ☐ | ☐ | _____ |
| 18 | ☐ | ☐ | ☐ | ☐ | _____ | 43 | ☐ | ☐ | ☐ | ☐ | _____ | 68 | ☐ | ☐ | ☐ | ☐ | _____ |
| 19 | ☐ | ☐ | ☐ | ☐ | _____ | 44 | ☐ | ☐ | ☐ | ☐ | _____ | 69 | ☐ | ☐ | ☐ | ☐ | _____ |
| 20 | ☐ | ☐ | ☐ | ☐ | _____ | 45 | ☐ | ☐ | ☐ | ☐ | _____ | 70 | ☐ | ☐ | ☐ | ☐ | _____ |
| 21 | ☐ | ☐ | ☐ | ☐ | _____ | 46 | ☐ | ☐ | ☐ | ☐ | _____ | 71 | ☐ | ☐ | ☐ | ☐ | _____ |
| 22 | ☐ | ☐ | ☐ | ☐ | _____ | 47 | ☐ | ☐ | ☐ | ☐ | _____ | 72 | ☐ | ☐ | ☐ | ☐ | _____ |
| 23 | ☐ | ☐ | ☐ | ☐ | _____ | 48 | ☐ | ☐ | ☐ | ☐ | _____ | 73 | ☐ | ☐ | ☐ | ☐ | _____ |
| 24 | ☐ | ☐ | ☐ | ☐ | _____ | 49 | ☐ | ☐ | ☐ | ☐ | _____ | 74 | ☐ | ☐ | ☐ | ☐ | _____ |
| 25 | ☐ | ☐ | ☐ | ☐ | _____ | 50 | ☐ | ☐ | ☐ | ☐ | _____ | 75 | ☐ | ☐ | ☐ | ☐ | _____ |

THIS FORM MAY BE LOCALLY REPRODUCED